

CHAPTER 12

Computers and Society: Security and Privacy

While enjoying your breakfast, you read an offer for a crossword puzzle CD-ROM on the back of your cereal box. All you have to do is send two UPC labels and \$1 for processing and handling. You immediately cut out the order form and fill in your name, home address, e-mail address, and telephone number. Crossword puzzles are your favorite pastime!

Three weeks later the software arrives. While installing the software, you register the product online. The next day, the manufacturer sends you an e-mail message with a list of other entertainment software in which you might be interested. As time passes, you begin to receive increasingly more e-mail messages from vendors of game and entertainment software. In addition, you begin to receive brochures in the U.S. mail from various related sources. Then, you receive a call from one of the vendors. How did all these companies obtain your name, e-mail address, and telephone number?

With school starting soon, you decide to buy your semester books from the campus online bookstore. While placing your order, the advertisement banner on the bookstore's Web page reads, Click here for a 50 percent discount on entertainment software. Is the content of this message a coincidence?



COMPUTER SECURITY: RISKS AND SAFEGUARDS

OBJECTIVES

After completing this chapter, you will be able to:

- Identify the various types of security risks that can threaten computers
- Describe ways to safeguard a computer
- Know how a computer virus works and the steps individuals can take to prevent viruses
- Understand how to create a good password
- Identify various biometric devices
- Recognize that software piracy is illegal
- Explain why encryption is necessary
- Know why computer backup is important and how it is accomplished
- Discuss the steps in a disaster recovery plan
- Understand ways to secure an Internet transaction
- List ways to protect your personal information

Today, more and more people rely on computers to create, store, and manage critical information. Thus, it is important that computers and the data they store are accessible and available when needed. It also is crucial that users take measures to protect their computers and data from loss, damage, and misuse. For example, businesses must ensure that information such as credit records, employee and customer data, and purchase information are secure and confidential.

A **computer security risk** is any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability. Some breaches to computer security are accidental. Others are planned. An intentional breach of computer security often involves a deliberate act that is against the law. Any illegal act involving a computer generally is referred to as a **computer crime**. The term **cybercrime** refers to online or Internet-based illegal acts.

The following sections describe some of the more common computer security risks and protective measures, or **safeguards**, you can take to minimize or prevent their consequences. This section concludes with a discussion of how to develop an overall computer security plan.

Computer Viruses

A computer **virus** is a potentially damaging computer program that affects, or *infects*, your computer negatively by altering the way the computer works without your knowledge or permission. More

specifically, a computer virus is a segment of program code from some outside source that implants itself in a computer. Once the virus is in your computer, it can spread throughout and may damage your files and operating system.

The increased use of networks, the Internet, and e-mail has accelerated the spread of computer viruses. With these technologies, computer users easily can share files and any related viruses. Viruses are activated on your computer in three basic ways: (1) opening an infected file, (2) running an infected program, or (3) booting the computer with an infected floppy disk in the disk drive.

Today, the most common way that computers become infected with viruses is through e-mail attachments. Figure 12-1 shows how a virus can spread from one computer to another through an infected e-mail attachment. Before you open or execute any e-mail attachment, you should ensure that the e-mail message is from a trusted source. A **trusted source** is a company or person you believe will not send you a virus-infected file knowingly. If the e-mail is from an unknown source, you should delete it without opening or executing any attachments. Following this precautionary measure will help protect your computer from virus infection.

Computer viruses do not generate by chance. The programmer of a virus, known as a **virus author**, intentionally writes a virus program. Some virus authors find writing viruses a challenge. Others write them to cause destruction. Writing a virus program usually requires significant programming skills. If virus authors would devote their time, energy, and skills to more productive activities, they most certainly could earn a substantial amount of honest money.

Web Link

For more information on computer viruses, visit the Discovering Computers 2002 Chapter 12 WEB LINK page (scsite.com/dc2002/ch12/weblink.htm) and click Computer Viruses.

Figure 12-1 HOW A VIRUS CAN SPREAD THROUGH AN E-MAIL MESSAGE**Step 1:**

Unscrupulous programmers create a virus program. They hide the virus in a Word document and attach the Word document to an e-mail message.

Step 2:

They use the Internet to send the e-mail message to thousands of users around the world.

**Step 3b:**

Other users do not recognize the name of the sender of the e-mail message. These users do not open the e-mail message — instead they immediately delete the e-mail message. These users' computers are not infected with the virus.

Step 3a:

Some users open the attachment and their computers become infected with the virus.

Some viruses are harmless pranks that simply freeze a computer temporarily or display sounds or messages. The Music Bug virus, for example, instructs the computer to play a few chords of music. Other viruses destroy or corrupt data stored on the hard disk of the infected computer. If your computer acts differently from usual, it may be infected with a virus. Figure 12-2 outlines some common symptoms of virus infection.

Viruses have become a serious problem in recent years. Currently, more than 53,000 known virus programs exist with an estimated 6 new virus programs discovered each day. Many Web sites maintain lists of all known virus programs.

Although numerous variations are known, three main types of viruses exist: boot sector, file, and macro.

- A **boot sector virus**, sometimes called a **system virus**, executes when a computer boots up because it resides in the boot sector of a floppy disk or the master boot record of a hard disk. When you leave a floppy disk in the floppy

disk drive and boot up the computer, the computer attempts to execute the boot sector on the disk in drive A. Even if the disk is not a boot disk, any virus on the floppy disk's boot sector can infect the computer's hard disk.

- A **file virus**, sometimes called a **program virus**, attaches itself to program files. When you run the infected program, the virus loads into memory. Most users innocently obtain a file virus by downloading a program from the Web or opening an e-mail attachment.
- A **macro virus** uses the macro language of an application, such as word processing or spreadsheet, to hide virus code. When you open a document that contains an infected macro, the virus loads into memory. The creators of macro viruses often hide them in templates, so the virus infects any document that uses the template.

Many viruses activate as soon as a computer accesses an infected file or runs an infected program. Other viruses, called logic bombs or time bombs, activate based on specific

criterion. A **logic bomb** is a virus that activates when it detects a certain condition. One disgruntled worker, for example, planted a logic bomb that began destroying files when his name appeared on a list of terminated employees. A **time bomb** is a type of logic bomb that activates on a particular date. A well-known time bomb is the Michelangelo virus, which destroys data on a hard disk on March 6, Michelangelo's birthday.

Viruses sometimes are called malicious-logic programs. A **malicious-logic program**, or **malware**, is a program that acts without a user's knowledge and deliberately alters the computer's operations. In addition to viruses, other types of malware are worms and Trojan horses.

- A **worm** is a malicious-logic program that copies itself repeatedly in memory or on a disk drive until no memory or disk space remains. When no memory or disk space remains, the computer stops working. Some worm programs even copy themselves to other computers on a network.
- A **Trojan horse** (named after the Greek myth) is a malicious-logic program that hides within or looks like a legitimate program. A certain condition or action usually triggers the Trojan horse. Unlike a virus or worm, a Trojan horse does not replicate itself to other computers.

SIGNS OF VIRUS INFECTION

- An unusual message or graphical image displays on the computer monitor
- An unusual sound or music plays randomly
- The available memory is less than what should be available
- A program or file suddenly is missing
- An unknown program or file mysteriously appears
- The size of a file changes without explanation
- A file becomes corrupted
- A program or file does not work properly

Figure 12-2 Viruses attack computers in a variety of ways. Listed here are some of the more common signs of virus infection.

Virus Detection and Removal

No completely effective methods exist to ensure a computer or network is safe from computer viruses and other malware. You can take precautions, however, to protect your home and work computers from these infections. The following paragraphs discuss these precautions.

To reduce the chance of infecting your computer with a boot sector virus, never start your computer with a floppy disk in drive A — unless you are certain the disk is an uninfected boot disk. All floppy disks contain a boot sector. During the startup process, the computer attempts to execute the boot sector on a disk in drive A. Even if the attempt is unsuccessful, any virus on the floppy disk's boot sector can infect the computer's hard disk.

To protect your computer from a macro virus, you can set a macro's security level in all applications that allow you to write macros. With a medium security level, for example, Microsoft Word will warn you that a document you are attempting to open contains a macro (Figure 12-3). From this warning, you can choose to disable or enable the macro. If the document is from a trusted source, you can enable the macro. Otherwise, you should disable it.

To safeguard your computer from virus attacks, install an antivirus program and update it frequently. An **antivirus program** protects a computer against viruses by identifying and removing any computer viruses found in memory, on storage media, or on incoming files. Most antivirus programs also protect against worms and Trojan horses. When you purchase a

new computer, it often includes an antivirus software package. The table in Figure 12-4 lists popular antivirus software packages.

POPULAR ANTIVIRUS SOFTWARE PACKAGES

- AVG Anti-Virus
- Command AntiVirus
- eSafe Desktop
- F-Secure Anti-Virus
- InoculateIT
- McAfee VirusScan
- Norton AntiVirus
- PC-cillin
- RAV AntiVirus Desktop

Figure 12-4 Popular antivirus software packages.

Figure 12-3a (dialog box to set macro security)

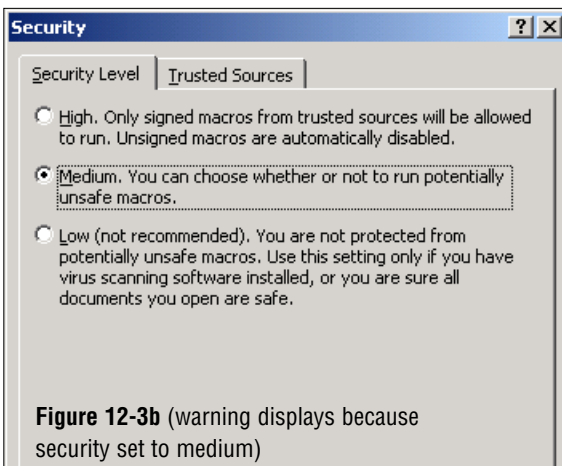


Figure 12-3b (warning displays because security set to medium)

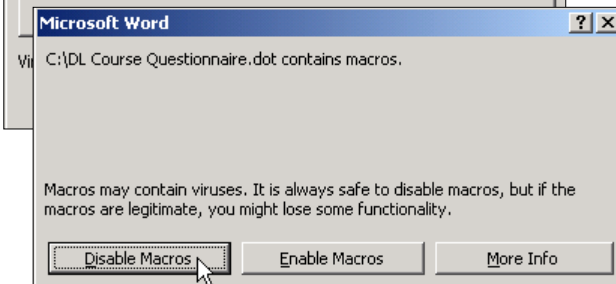


Figure 12-3 Many application software products, such as Microsoft Word, allow you to set security levels for macros. To display the dialog box shown in Figure 12-3a in Word, click Tools on the menu bar, point to Macro, and then click Security.

COMPANY ON THE CUTTING EDGE



Antivirus Program Provides Personal Computer Protection

Some people take megadoses of Vitamin C to fight a cold. Others rely on homemade chicken soup to eliminate viral infections. But how can they protect their computers from viral attacks? Their best bet is to use a combination of an antivirus program and a personal firewall, such as McAfee VirusScan and Firewall, developed by Network Associates.

More than 53,000 strains of viruses are on the rampage to infect your system with Trojan horses, worms, and bugs. But Network Associates' cybersleuths are on the lookout for these malicious programs, sometimes finding as many as six new viruses each day. They are part of the company's 2,800 worldwide employees and the largest independent network security and management software corporation.

VirusScan has been named the top antivirus product in independent testing performed by the University of Hamburg's Virus Test Center and by the West Coast Labs for Secure Computing. This software, along with Network Associates' other e-business products, is used by more than 60 million people worldwide.

For more information on Network Associates, Inc., visit the Discovering Computers 2002 Companies Web page (sccsite.com/dc2002/companies.htm) and click Network Associates.

An antivirus program scans for programs that attempt to modify the boot program, the operating system, and other programs that normally are read from but not modified. Many antivirus programs also automatically scan files you download from the Web, e-mail attachments, files you open, and all removable media you insert into the computer such as floppy disks and Zip® disks.

One technique that antivirus programs use to identify a virus is to look for virus signatures. A **virus signature**, also called a **virus definition**, is a known specific pattern of virus code. You should update your antivirus program's signature files as often as necessary to ensure these files contain patterns for newly discovered viruses. This extremely important activity allows your antivirus software to protect against viruses written since the antivirus program was released. Most antivirus programs contain an auto-update feature that regularly prompts you to download the virus signature (Figure 12-5). The vendor usually provides this service at no cost for a specified time period.

Even with an updated virus signature file, antivirus programs can have difficulty detecting some viruses. For example, a **polymorphic virus** modifies its program code each time it attaches itself to another program or file. An antivirus program cannot detect a polymorphic virus by its virus signature because the code pattern in the virus never looks the same.

Another technique that antivirus programs use to detect viruses is to inoculate existing program files. To **inoculate** a program file, the antivirus program records information such as the file size and file creation date in a separate inoculation file. The antivirus program then can use this information to detect if a virus tampers with the inoculated program file. Again, some sophisticated viruses take steps to avoid detection. A **stealth virus** infects a program file, but still reports the size and creation date of the original, uninfected program.

Once an antivirus program identifies an infected file, it attempts to remove its virus. If the antivirus program cannot remove the virus, it often quarantines the infected file.

A **quarantine** is a separate area of a hard disk that holds the infected file until you can remove its virus. This step ensures other files will not become infected. You also can quarantine suspicious files yourself.

In addition to detecting and inoculating against viruses, most antivirus programs have utilities that create a rescue disk and remove or repair infected programs and files. For boot sector viruses, the antivirus program requires you to restart the computer with a rescue disk. The **rescue disk**, or **emergency disk**, is a removable disk that contains an uninfected copy of key operating system commands and startup information that enables the computer to restart correctly. Upon startup, the rescue disk finds and removes the boot sector virus. Floppy disks and Zip® disks often serve as rescue disks. Once you have restarted the computer using the rescue disk, the antivirus program can attempt to repair damaged files. If it cannot repair the damaged files, you may have to replace, or *restore*, them with uninfected backup copies of the files.

In extreme cases, you may need to reformat your hard disk to remove a virus. Having uninfected, or clean, backups of all files is important. A later section in this chapter covers backup and restore procedures in detail.

If a virus has infected your computer, you should remove the virus. If you share data with other users, such as via e-mail attachments, floppy disks, or Zip® disks, then you should inform these users of your virus infection. This courteous gesture allows fellow users to check their system for the same virus infection.

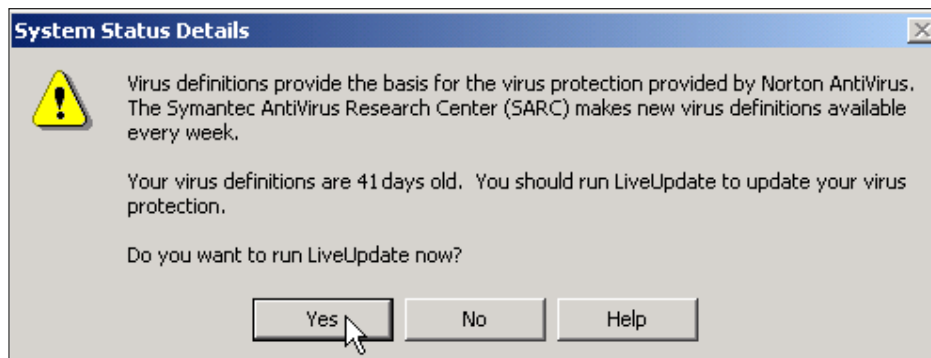


Figure 12-5 Many vendors of antivirus programs allow you to update virus signature files automatically from the Web at no cost for a specified time period.

Finally, stay informed about new virus alerts and virus hoaxes. A **virus hoax** is an e-mail message that warns you of a non-existent virus. Often, these virus hoaxes are in the form of a chain letter that requests you send a copy of the e-mail to as many people as possible. Instead of forwarding the e-mail, visit a Web site that publishes a list of virus alerts and virus hoaxes (Figure 12-6).

The list in Figure 12-7 summarizes important tips discussed in this section for protecting your computer from virus infection.

Unauthorized Access and Use

Unauthorized access is the use of a computer or network without permission. A **cracker** is someone who tries to access a computer or network illegally. The term **hacker**, although originally a complimentary word for a computer enthusiast, now has a derogatory connotation with the same definition as cracker. Some hackers break into a computer for the challenge. Other hackers use or steal computer resources or corrupt a computer's data.

Hackers typically break into a computer by connecting to it and then logging in as a legitimate user. Some intruders do no damage. They merely access data, information, or programs on the computer before logging off. Other intruders leave some evidence of their presence either by leaving a message or deliberately altering data.

Unauthorized use is the use of a computer or its data for unapproved or possibly illegal activities. Unauthorized use includes a variety of activities: an employee using a company computer to send personal e-mail, an employee using the company's word processing software to track his or her child's soccer league scores, or someone gaining access to a bank computer and performing an unauthorized transfer.

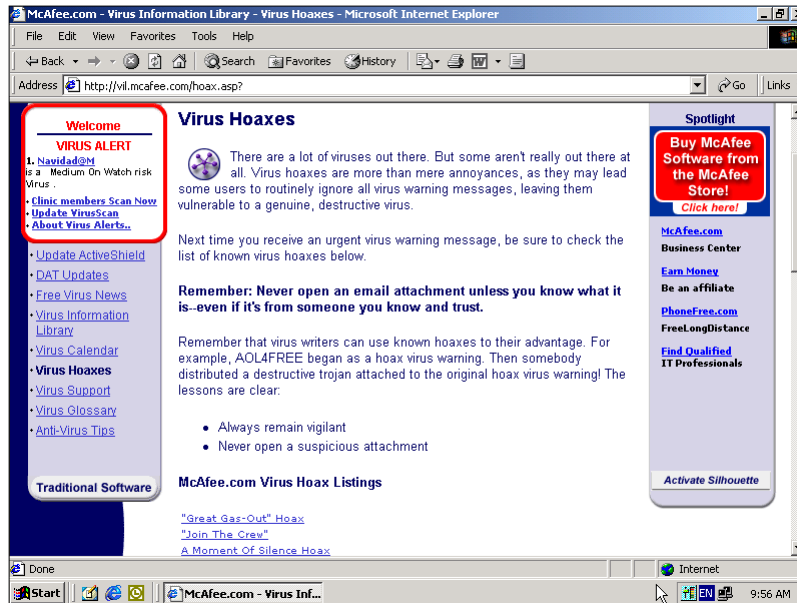


Figure 12-6 Stay informed of virus alerts and hoaxes by regularly visiting a Web site such as the one shown here.

TIPS FOR PREVENTING VIRUS INFECTIONS

1. Never start your computer with a floppy disk in drive A, unless it is an uninfected rescue disk.
2. Set the macro security in programs so you can enable or disable macros. Only enable macros if the document is from a trusted source.
3. Install an antivirus program on all of your computers. Obtain updates to the antivirus signature files. The cost of antivirus software is much less than the cost of rebuilding damaged files. As a result, most businesses and large organizations have adopted this policy.
4. If your antivirus program flags an e-mail attachment as virus infected, delete the attachment immediately. Never open an e-mail attachment unless it is from a trusted source. Scan all e-mail attachments you intend to open.
5. Check all downloaded programs for viruses. Viruses often are placed in seemingly innocent programs so they will affect a large number of users.
6. Before using any floppy disk or Zip® disk, use the antivirus scan program to check the disk for viruses. This holds true even for shrink-wrapped software from major developers. Even commercial software has been infected and distributed to unsuspecting users.
7. Write-protect your rescue disk by sliding the write-protect tab into the write-protect position.
8. Back up your files regularly. Scan the backup program prior to backing up disks and files to ensure the backup program is virus free.

Figure 12-7 With the growing number of new viruses, it is crucial you take steps to protect your computer. Experts recommend the precautions listed here.

TECHNOLOGY TRAILBLAZER

CLIFFORD STOLL

Technology Trailblazers have invented computer hardware, developed computer software, changed the way individuals and organizations use computers, and led prominent companies in the computer industry. Clifford Stoll, however, does not create computer technology. Instead, Stoll provokes people to *think* about how they use computer technology.

Stoll first gained fame working as a systems manager at Lawrence Berkeley National Laboratory, managed by the University of California for the U.S. Department of Energy. While tracking the source of a 75-cent accounting error in his company's billing logs, he noticed something awry. After a year of thorough investigation — done solely from his computer — Stoll finally tracked the hacker to Hanover, West Germany. The hacker turned out to be part of a spy ring selling computer secrets to the Soviet Union's KGB for money and drugs. The details of this pursuit are revealed in Stoll's 1989 book, *The Cuckoo's Egg*, which made *The New York Times*' bestseller list.

He also wrote two other books, *Silicon Snake Oil — Second Thoughts on the Information Highway* and *High Tech Heretic: Why Computers Don't Belong in the Classroom*. As these titles suggest, Stoll is highly critical of the benefits computers and the Internet presumably provide. He questions why computers are so bland looking and why hardware has such a short useful life, and he proclaims that schools should spend money on teachers, librarians, and books rather than on technology because computers tend to isolate and weaken people.

For more information on Clifford Stoll, visit the Discovering Computers 2002 People Web page (scsite.com/dc2002/people.htm) and click Clifford Stoll.



One way to prevent unauthorized access and unauthorized use of computers is to utilize access controls. An **access control** is a security measure that defines who can access a computer, when they can access it, and what actions they can take while accessing the computer. Many commercial software packages implement access controls using a two-phase process called identification and authentication. **Identification** verifies that you are a valid user. **Authentication** verifies that you are whom you claim to be. Four methods of identification and authentication exist: user names and passwords, possessed objects, biometric devices, and callback systems. The following pages discuss these methods of identification and authentication.

USER NAMES AND PASSWORDS A **user name**, or **user ID**, is a unique combination of characters, such as letters of the alphabet or numbers, that identifies one specific user. A **password** is a secret combination of characters associated with the user name that allows access to certain computer resources.

As discussed in Chapter 8, most multiuser (networked) operating systems require that you correctly enter a user name and a password before you can access the data, information, and programs stored on a computer or network. Many other systems that maintain financial, personal, and other confidential information also require a user name and password as part of their logon procedure (Figure 12-8).

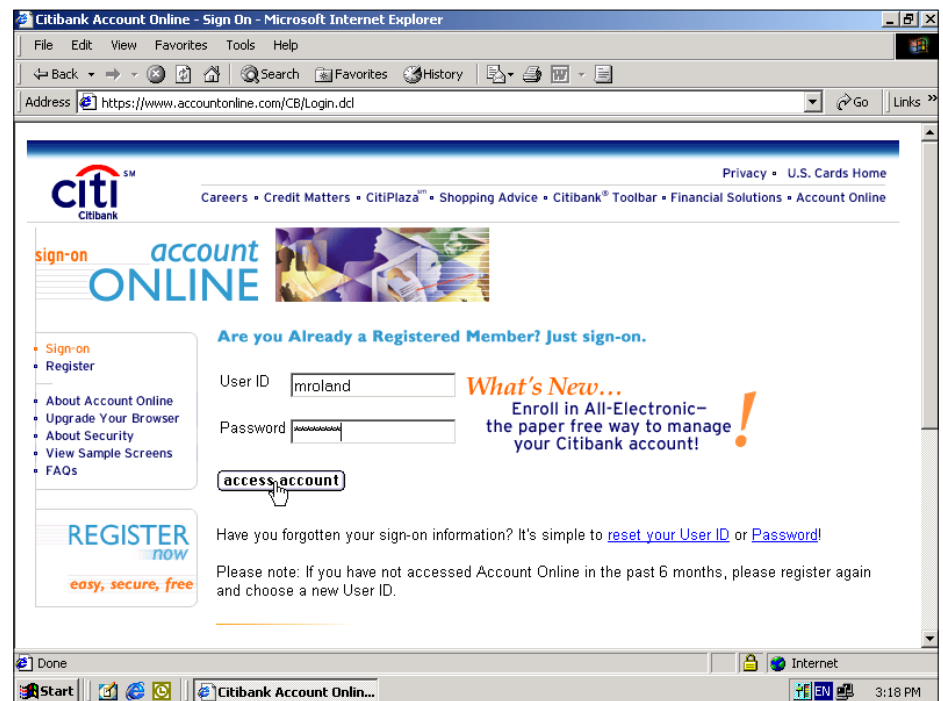


Figure 12-8 Many Web sites that maintain personal and confidential data require a user to enter a user name and password.



The Perfect Password

Accessing your computer account online, at school, or at work generally requires that you have a user name and password. Passwords are effective, however, only if they are chosen carefully. Ideally, the password should be one that nobody could guess. In practice, most people select passwords that are easy to guess: their name or their initials, or names of their children, spouse, or pets.

Below are some tips on selecting a password.

Do not use:

- Your name in any form.
- The name of a family member.
- A password of all digits or all the same letter.
- A password contained in an English or foreign language dictionary.

Do use:

- At least eight characters (if supported by the software).
- Mixed case letters.
- A combination of letters, digits, words, initials, and dates.
- The license plate rule (characters you would use to create a personal license plate).
- A password you can type easily without looking at the keyboard.
- Something that no one but you would know.
- A line or two from a song, using the first letter of each word.

Below are some tips on safeguarding your password:

- Do not share your password with anyone.
- Do not write down your password.
- Change your password frequently.
- Do not fall for e-mail or telephone scams and share your password.

For more information on password protection, visit the Discovering Computers 2002 Apply It Web page (sccsite.com/dc2002/apply.htm) and click Chapter 12 Apply It #1.

Some systems assign your user name or user identification (ID). For example, a school may use your student identification number as your user ID. With other systems, you select your own user name. Many users select a mixture of their first and last names. A user named Michael Roland might choose mroland as his user name.

Most systems require you to select your own password. Users typically choose an easy-to-remember word or series of characters for passwords. If your password is too obvious, however, such as your initials or birthday, others can guess it easily. Easy passwords make it simple for hackers to break into a system. Thus, you should select a password carefully.

Longer passwords provide greater security than shorter ones. Each character you add to a password significantly increases the number of possible combinations and the length of time it might take for someone to guess the password (Figure 12-9).

Generally, the more creative you are when selecting a password, the more difficult it is for someone to figure out.

PASSWORD PROTECTION

NUMBER OF CHARACTERS	POSSIBLE COMBINATIONS	AVERAGE TIME TO DISCOVER	
		HUMAN	COMPUTER
1	36	3 minutes	.000018 second
2	1,300	2 hours	.00065 second
3	47,000	3 days	.02 second
4	1,700,000	3 months	1 second
5	60,000,000	10 years	30 seconds
10	3,700,000,000,000,000	580 million years	59 years

- Possible characters include the letters A-Z and numbers 0-9
- Human discovery assumes 1 try every 10 seconds
- Computer discovery assumes one million tries per second
- Average time assumes the password would be discovered in approximately half the time it would take to try all possible combinations

Figure 12-9 This table shows the effect of increasing the length of a password that consists of letters and numbers. The longer the password, the more effort required to discover it. Long passwords, however, are more difficult for users to remember.

Many software programs have guidelines you must follow when you create your password. One system may require your password be at least six characters long and use a mixture of numbers and letters. Following these guidelines, the password IAWL is invalid (it is too short), but IAWL0901 is valid. This password also is easy for you to remember because the letters IAWL are the first letter of each word in your favorite movie, *It's a Wonderful Life*, and September 1 is your anniversary (09/01). Although easy for you to remember, this password is difficult for a hacker to guess easily.

To provide even more protection, some systems ask users to enter one of several pieces of personal information. The question is chosen randomly from information on file. Such items can include a spouse's first name, a birth date, a place of birth, or a mother's maiden name. As with a password, if the user's response does not match the information on file, the system denies access.

Web Link

For more information on personal identification numbers, visit the Discovering Computers 2002 Chapter 12 WEB LINK page (scsite.com/dc2002/ch12/weblink.htm) and click Personal Identification Numbers.

POSSESSED OBJECTS A **possessed object** is any item that you must carry to gain access to a computer or computer facility. Examples of possessed objects are badges, cards, and keys. The card you use in an automated teller machine (ATM) is a possessed object that allows access to your bank account (Figure 12-10).

Possessed objects often are used in combination with personal identification numbers. A **personal identification number (PIN)** is a numeric password, either assigned by a company or selected by you. PINs provide an additional level of security. An ATM card typically requires a four-digit PIN. If someone steals your ATM card, the thief must enter your PIN to access your bank account. PINs are passwords. Select them carefully and protect them as you do any other password.

BIOMETRIC DEVICES A **biometric device** authenticates a person's identity by verifying personal characteristics. These devices grant access to programs, systems, or rooms using computer analysis of some biometric identifier. A **biometric identifier** is a physical or behavioral characteristic. Examples include fingerprints, hand geometry, facial features, voice, signatures, and retinal (eye) patterns.

A biometric device translates a personal characteristic into a digital code that is compared to a digital code stored in the computer. If the digital code in the computer does not match the personal characteristics code, the computer denies access to the individual. Many types of biometric devices exist for computer security purposes.



Figure 12-10 The card you use in an automated teller machine (ATM) is a possessed object that allows access to your bank account.

The most widely used biometric device today is a fingerprint scanner. A **fingerprint scanner** captures curves and indentations of a fingerprint (Figure 12-11). With the cost of fingerprint scanners dropping to less than \$100, many believe this will become the home user's authentication device for e-commerce transactions.



Figure 12-11 Many people believe fingerprint scanners will become the home user's authentication device for e-commerce transactions.

To make a credit-card transaction, the Web site would require you hold your finger on the scanner. These devices usually plug into a parallel or USB port. To save on desk space, some newer keyboards and notebook computers have a fingerprint scanner built into them.

Biometric devices also can measure the shape and size of a person's hand using a **hand geometry system** (Figure 12-12). Costing more than \$1,000, larger companies typically use these systems as time and attendance devices. One university cafeteria uses a hand geometry system to verify students when they use their meal card. A day care center uses a hand geometry system to verify parents that pick up their children.



Figure 12-12 A user's identity can be verified by his or her hand with a hand geometry system.

A **face recognition system** captures a live face image and compares it to a stored image to determine if the person is a legitimate user (Figure 12-13). Some notebook computers use this security technique to safeguard the computer. The computer will not boot up unless the user is legitimate. These programs are becoming more sophisticated and can recognize people with or without glasses, makeup, or jewelry, and with new hairstyles.

Web Link

For more information on biometric devices, visit the Discovering Computers 2002 Chapter 12 WEB LINK page (scsite.com/dc2002/ch12/weblink.htm) and click Biometric Devices.



Figure 12-13 A face recognition system captures a live face image and compares it to a stored image to determine if the person is a legitimate user.

A **voice verification system** compares a person's live speech to their stored voice pattern. Larger organizations sometimes use voice verification systems as time and attendance devices. Many companies also use this technology for access to sensitive files and networks. Some financial services use voice verification systems to secure telephone banking transactions. These systems use speaker dependent voice recognition software. As discussed in Chapter 5, this type of software requires the computer to make a profile of your voice. That is, you train the computer to recognize your inflection patterns.

A **signature verification system** recognizes the shape of your handwritten signature, as well as measuring the pressure exerted and the motion used to write the signature. Signature verification systems use a specialized pen and tablet.

Extremely high-security areas use retinal scanners (Figure 12-14). An **iris recognition system** reads patterns in the tiny blood vessels in the back of the eye, which are as unique as a fingerprint. These systems are very expensive and are used by government security organizations, the military, and financial institutions that deal with highly sensitive data.

Biometric devices are gaining popularity as a security precaution because they are a virtually foolproof method of identification and authentication. Users can forget their user names and passwords. Possessed objects can be lost, copied, duplicated, or stolen. Personal characteristics, by contrast, are unique and cannot be forgotten or misplaced.

Biometric devices do have some disadvantages. If you cut your finger, a fingerprint scanner might reject you as a legitimate user. Hand geometry readers can transmit germs. If you are nervous, a signature might not match the one on file. If you have a sore throat, a voice recognition system might reject you. Many people are uncomfortable with the thought of using an iris scanner.

CALLBACK SYSTEM A callback system is an access control method that some systems utilize to authenticate remote users. With a **callback system**, you can connect to a computer only after the computer calls you back at a previously established telephone number.

To initiate the callback system, you call the computer and enter a user name and password. If these entries are valid, the computer instructs you to hang up and then calls you back. A callback system provides an additional layer of security. Even if a person steals or guesses a user name and password, that person also must be at the authorized telephone number to access the computer.

Callback systems work best for users who regularly work at the same remote location such as from home or a branch office. Mobile users that need to access a computer from different locations and telephone numbers can use a callback system, but they have to change the callback number stored by the callback system each time they move to a different location.



Figure 12-14 As this customer looks into the camera, an iris recognition system verifies her identity by comparing her iris structure with one stored in the computer. She only will be allowed to make a transaction if the system authenticates her as a valid user.

The authentication technique a company uses should correspond to the degree of risk associated with the unauthorized access. In addition, a company regularly should review users' authorization levels to determine if they still are appropriate.

No matter what type of identification and authentication techniques a company uses, the computer should maintain an **audit trail** or **log** that records in a file both successful and unsuccessful access attempts. Companies should investigate unsuccessful access attempts immediately to ensure they were not intentional breaches of security. They also should review successful access for irregularities, such as use of the computer after normal working hours or from remote computers.

In addition, companies should have written policies regarding the use of computers by employees for personal reasons. Some companies prohibit such use entirely. Others allow personal use on the employee's own time such as a lunch hour. Whatever the policy, a company should document and explain it to employees.

Hardware Theft

Hardware theft is the act of stealing computer equipment.

Hardware vandalism is the act of defacing or destroying computer equipment. For the desktop computer at home, hardware theft and vandalism usually are not a problem. Companies, however, must protect their computers and associated equipment from theft or vandalism.

To help reduce the chances of theft, companies can use a variety of security measures. Physical access controls, such as locked doors and windows, usually are adequate to protect the equipment. Many businesses, schools, and some homeowners also install alarm systems for additional security. School computer labs and other areas with a large number of semi-frequent users often utilize additional physical security devices such as cables that lock the equipment to a desk, cabinet, or floor (Figure 12-15).

With mobile equipment such as notebook and handheld computers, hardware theft poses a more serious risk. Increasingly, businesses and schools provide notebook computers to employees and students, in addition to loaning them out for short periods. Mobile computer users must take special care to protect their equipment. High-end notebook computers, some of which cost more than \$5,000, are particularly at risk. Their size and weight make them easy to steal, and their value makes them tempting targets for thieves.

Common sense and a constant awareness of the risk are the best preventive measures against theft of notebook computers and other mobile equipment. For example, you should

never leave a notebook computer unattended in a public place such as an airport or a restaurant or out in the open such as on the seat of a car. You also may want to use a physical device such as a cable to lock a mobile computer temporarily to a desk or table.

Some notebook computers use passwords, possessed objects, and biometrics as a method of security. When you boot up these computers, users must authenticate themselves before the password-protected hard disk unlocks. As discussed earlier, some use a face recognition system. Others use a fingerprint scanner, card, or other device. This type of security will not prevent theft, but it will render the computer useless if it is stolen. As a precaution in case of theft, you should back up the files stored on your notebook computer regularly.

For handheld computers, you also can password protect the device. This allows only authorized users access to its data. You usually can instruct the password screen to display your name and telephone number, so a Good Samaritan can return it to you if lost. Several models allow you to encrypt data in the device. A later section in this chapter discusses encryption.

In addition to hardware theft, another area of concern for businesses and schools is vandalism. Computer vandalism takes many forms, from someone cutting a computer cable or deleting important files, to individuals breaking in a business or school computer lab and randomly smashing computers. Most organizations have written policies and procedures for dealing with the various types of vandalism.



Figure 12-15 Using cables to lock computers can help prevent the theft of desktop and mobile computer equipment.

Software Theft

As with hardware theft and vandalism, software theft can take many forms — from someone physically stealing media that contains software, such as a DVD-ROM, CD-ROM, Zip® disk, or floppy disk, to intentional piracy of software.

Software piracy is the unauthorized and illegal duplication of copyrighted software. Software piracy is by far the most common form of software theft.

When you purchase software, you do not *own* the software. Instead, you become a licensed user. You obtain a **license agreement**, or the right to use the software. The license agreement provides specific conditions for use of the software, which a user must accept before using the software (Figure 12-16). You often can see the terms of a license agreement through the shrink wrap surrounding purchased software. In addition, these terms usually display when you install the software. In the case of software on the Web, the terms display on a page at the manufacturer's Web site. Use of the software constitutes acceptance of the terms on the user's part.

Web Link

For more information on software piracy, visit the Discovering Computers 2002 Chapter 12 WEB LINK page (scsite.com/dc2002/ch12/weblink.htm) and click Software Piracy.

The most common type of license included with software packages purchased by individual users is a **single-user license agreement**, also called an **end-user license agreement (EULA)**. A single-user license agreement typically includes many of the following conditions that specify a user's responsibility upon acceptance of the agreement.

Users are permitted to:

- Install the software on only one computer.
- Make one copy for backup.
- Give or sell the software to another individual, but only if they remove the software from their computer first.

Users are not permitted to:

- Install the software on a network, such as a school computer lab.
- Give copies to friends and colleagues.
- Export the software.
- Rent or lease the software.

Unless otherwise specified by a license agreement, you do not have the right to copy, loan, rent, or in any way distribute the software. Doing so is a violation of copyright law. It also is a federal crime. Despite this, experts estimate for every authorized copy of software in use, at least one unauthorized copy exists. One study reported software piracy results in worldwide sales losses of more than \$11 billion per year.

Software piracy continues for several reasons. In some countries, legal protection for software does not exist. In other countries, laws rarely are enforced. In addition, many buyers believe they have the right to copy the software for which they pay hundreds, even thousands of dollars. Finally, particularly in the case of removable media such as Zip® disks and floppy disks, software piracy is a simple crime to commit.

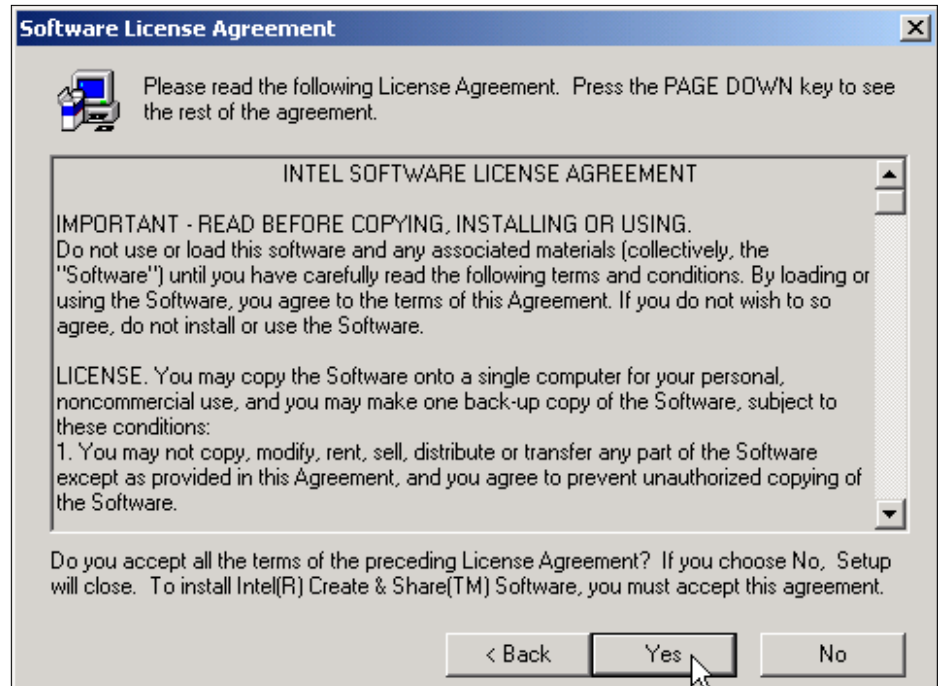


Figure 12-16 You must accept the terms in the license agreement before using the software.

Software piracy, however, is a serious offense. For one, it introduces a number of risks into the software market. It increases the chance of viruses, reduces your ability to receive technical support, and significantly drives up the price of software for all users. Further, software companies take illegal copying seriously. In some cases, offenders have been prosecuted to the fullest extent of the law with penalties including fines up to \$250,000 and five years in jail.

To promote a better understanding of software piracy problems and, if necessary, to take legal action, a number of major U.S. software companies formed the **Business Software Alliance (BSA)**. BSA operates a Web site (Figure 12-17) and antipiracy hotlines in the United States and more than 60 other countries.

Many organizations and businesses also have strict written policies governing the installation and use of software and enforce their rules by periodically checking networked or online computers to ensure that all software is licensed properly. If you

are not completely familiar with your school or employer's policies governing installation of software, you always should check with the information technology department or your school's technology coordinator.

To help reduce the software costs for companies with large numbers of users, software vendors often offer them special discount pricing. The more copies of a program a company purchases, the greater the discount. A software **site license** gives the buyer the right to install the software on multiple computers at a single site. Site license fees usually cost significantly less than purchasing individual copies of software for each computer.

Many software packages also have network versions. A **network site license** allows network users to share a single copy of the software, which resides on the network server. Software companies typically price network software site licenses based either on a fixed fee for an unlimited number of users, a maximum number of users, or on a per-user basis.

Information Theft

Information is a valuable asset to a company. **Information theft** occurs when someone steals personal or confidential information. If stolen, the loss of information can cause as much damage as (if not more than) the theft of hardware or software.

Both business and home users can fall victim to information theft. A company may steal or buy stolen information to learn about a competitor. An individual may steal credit card numbers to make fraudulent purchases. Information theft often is linked to other types of computer crime. An individual might first gain unauthorized access to a computer and then steal credit card numbers stored in a firm's accounting department.

Most companies attempt to prevent information theft by implementing the user identification and authentication controls discussed earlier in this chapter. These controls are best suited for protecting information on computers located on a company's premises. Information transmitted over networks offers a higher degree of risk because unscrupulous users can intercept it during transmission.

One way to protect sensitive data is to encrypt it. The following section discusses encryption techniques.

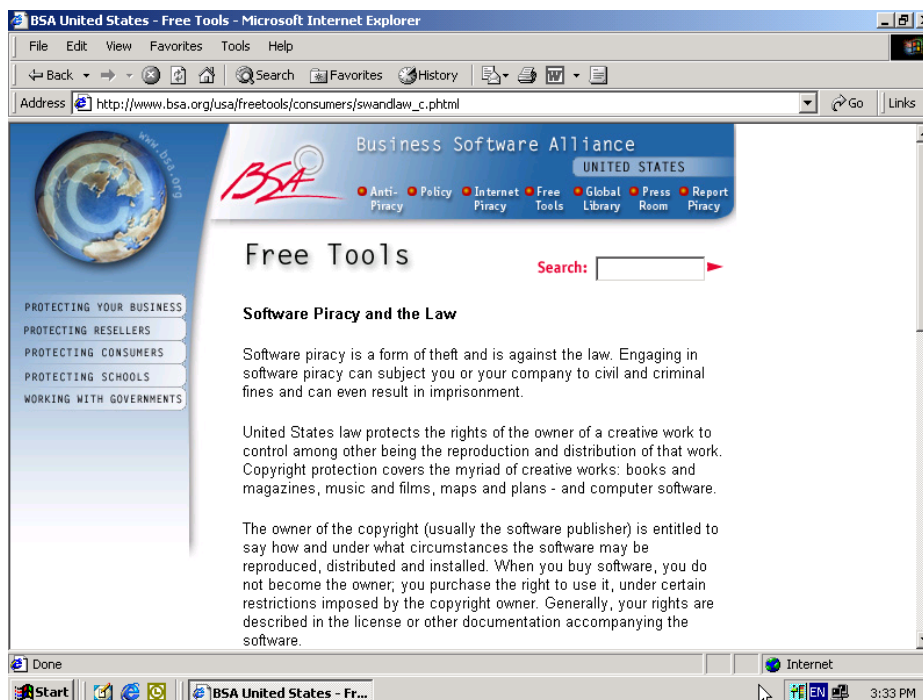


Figure 12-17 The Business Software Alliance (BSA) Web site provides the latest information about software piracy.

Web Link

For more information on the Business Software Alliance, visit the Discovering Computers 2002 Chapter 12 WEB LINK page (scsite.com/dc2002/ch12/weblink.htm) and click Business Software Alliance.

ENCRYPTION **Encryption** is the process of converting readable data into unreadable characters to prevent unauthorized access. You treat encrypted data just like any other data. That is, you can store it or send it in an e-mail message. To read the data, the recipient must **decrypt** it, or decipher it into a readable form.

In the encryption process, the unencrypted, readable data is called **plaintext**. The encrypted (scrambled) data is called **ciphertext**. To encrypt the data, the originator of the data

converts the plaintext into ciphertext using a password or an encryption key. In its simplest form, an **encryption key** is a formula that the recipient of the data uses to decrypt ciphertext.

Many data encryption methods exist. Figure 12-18 shows examples of some simple encryption methods. Figure 12-19 shows a sample encrypted file. An encryption key (formula) often uses more than one of these methods, such as a combination of transposition and substitution. Most organizations use available

software packages for encryption. Others develop their own encryption programs.

The two basic types of encryption are private key and public key. With **private key encryption**, also called a **symmetric key encryption**, both the originator and recipient use the same secret key to encrypt and decrypt the data. The most popular private key encryption system is the **data encryption standard (DES)**. The U.S. government is a primary user of the DES.

SIMPLE ENCRYPTION METHODS

NAME	METHOD	PLAINTEXT	CIPHERTEXT	EXPLANATION
Transposition	Switch the order of characters	WIRELESS	IWERELSS	Adjacent characters swapped
Substitution	Replace characters with other characters	LAPTOP	XDQORQ	Each letter replaced with another
Expansion	Insert characters between existing characters	MOUSE	MDODUDSDED	Letter D inserted after each character
Compaction	Remove characters and store elsewhere	COMMUNICATION	COMUICTIN	Every third letter removed (M, N, A, O)

Figure 12-18 This table shows four simple methods of encryption, the process of translating plaintext into ciphertext. Most encryption programs use a combination of these four methods.

Web Link

For more information on encryption, visit the Discovering Computers 2002 Chapter 12 WEB LINK page (scs.site.com/dc2002/ch12/weblink.htm) and click Encryption.



Figure 12-19 A sample encrypted file.

Public key encryption, also called **asymmetric key encryption**, uses two encryption keys: a public key and a private key. Public key encryption software generates both your private key and public key. A message encrypted with your public key only can be decrypted with your private key, and vice-versa.

The public key is made known to those with which you communicate. For example, public keys are posted on a Web page or e-mailed. In other cases, a central administrator publishes a list of public keys on a public-key server. The private key, by contrast, is kept confidential. Never share your private key with anyone nor send it over the Internet for any reason.

To send an encrypted e-mail message with public key encryption, the sender uses the receiver's public key to encrypt the message. Then the receiver uses his or her private key to decrypt the message (Figure 12-20). For example, if Joan wants to send

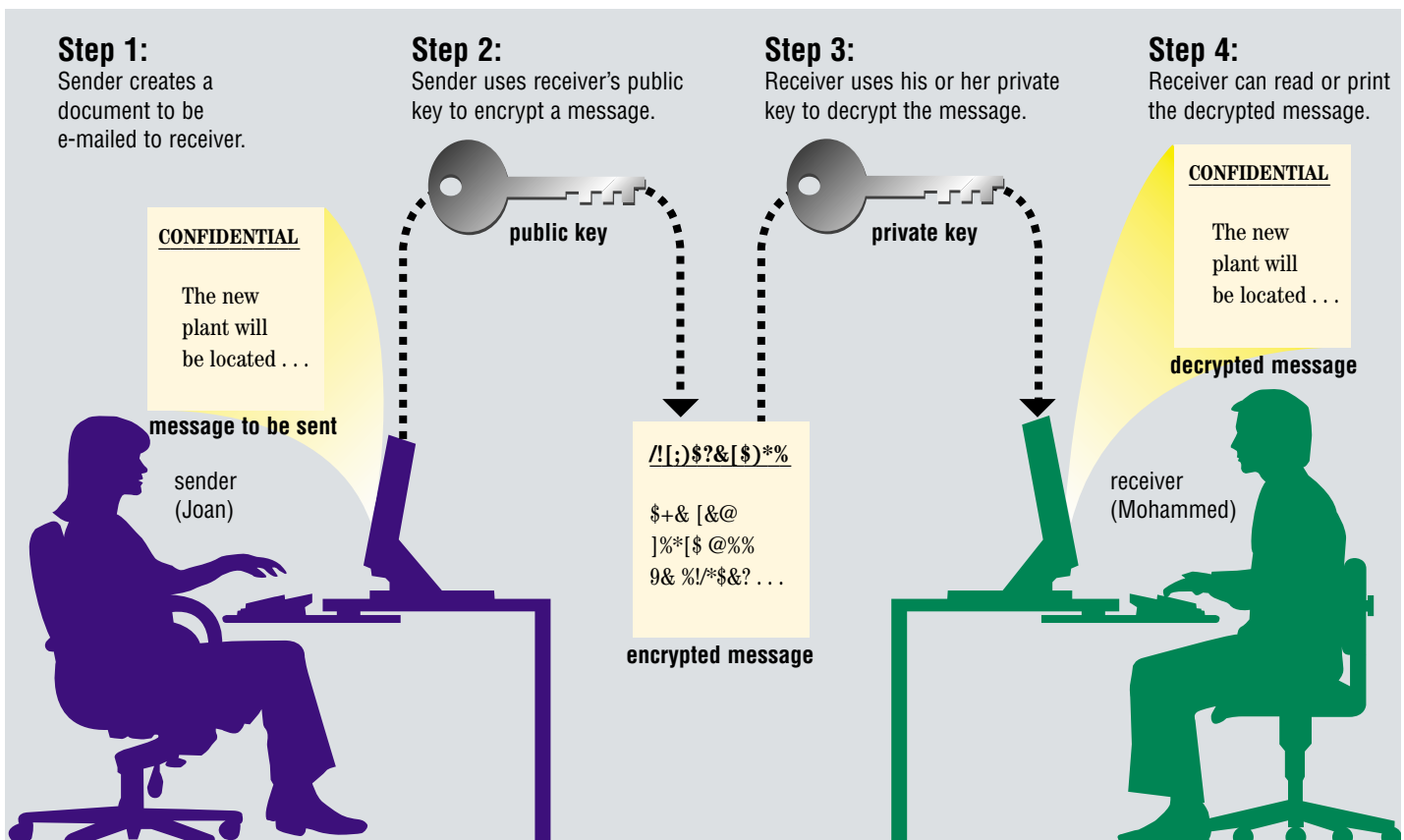
Mohammed an encrypted message, she would use Mohammed's public key to encrypt the message. When Mohammed receives the encrypted message, he would use his private key to decrypt it. Mohammed's encryption software generated his public and private keys. Joan used Mohammed's public key to encrypt the message. Thus, only Mohammed will be able to decrypt the message with his private key.

RSA encryption, named from its inventors, Rivest, Shamir, and Adleman, is a powerful public key encryption technology used to encrypt data transmitted over the Internet. Many software and public key encryption programs use RSA technology. Examples include Pretty Good Privacy (PGP) and newer versions of Netscape Navigator and Microsoft Internet Explorer.

Fortezza is another public key encryption technology that stores the user's private key and other information on a PC Card.

Since 1993, the United States government has proposed several ideas for developing a standard for voice and data encryption that would enable government agencies, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI), to monitor private communications as ordered through court decree. An early government proposal used an encryption formula in a tamper-resistant personal computer processor called the **Clipper chip**. Widespread opposition to this hardware approach caused the idea to be abandoned. In its place, the government proposed a key escrow plan, similar to the public key encryption method. The government's **key escrow** plan proposed using independent escrow organizations that would have custody of private keys that could decode encrypted messages. If necessary, authorized government agencies could obtain the necessary key. This plan also has been opposed and has not yet been implemented.

Figure 12-20 AN EXAMPLE OF PUBLIC KEY ENCRYPTION



ISSUE

Secret Code on the Internet?

Data Encryption

Encryption is technology that encodes computer files and communications, much as a combination lock secures a filing cabinet. Internationally, encryption products are widely available. The Freedom system, a new product from Zero-Knowledge Systems (see URL below), strips identifying information from e-mail and makes it impossible to track Web surfing habits. Consumer advocates and civil libertarians praise the new product, but police officers and Internet lawyers are wary. Freedom's encryption techniques can camouflage people participating in illegal activities on the Internet, such as child pornography or software piracy. Law enforcement officials insist that Freedom should allow them, when they have proof a crime has been committed, to trace Freedom users. To what extent is online anonymity a desirable trait? Why? Should there be limits to online anonymity? Why or why not? Should data encryption techniques be available without limit around the world? What about their antisocial uses by criminals?

For more information on encryption and privacy and the Web site mentioned above, visit the Discovering Computers 2002 Issues Web page (scs.site.com/dc2002/issues.htm) and click Chapter 12 Issue #1.

Web Link

For more information on surge protectors, visit the Discovering Computers 2002 Chapter 12 WEB LINK page (scs.site.com/dc2002/ch12/weblink.htm) and click Surge Protectors.

System Failure

Theft is not the only cause of hardware, software, data, or information loss. A **system failure**, which is the prolonged malfunction of a computer, also can cause loss of hardware, software, data, or information. A variety of causes can lead to system failure. These include aging hardware; natural disasters such as fires, floods, or storms; and random events such as electrical power problems.

One of the more common causes of system failure is an electrical power variation. Electrical power variations can cause loss of data or loss of equipment. If the computer equipment is networked, a single power disturbance can damage multiple systems. Electrical disturbances include noise, undervoltages, and overvoltages.

Noise is any unwanted signal, usually varying quickly, that is mixed with the normal voltage entering the computer. Noise is caused by external devices such as fluorescent lighting, radios, and televisions, as well as from components within the computer itself. Noise generally is not a risk to hardware, software, or data. Computer power supplies, however, do filter out noise.

An **undervoltage** occurs when the electrical supply drops. In North America, electricity normally flows from the wall plug at approximately 120 volts. Any significant drop below 120 volts is an undervoltage. A **brownout** is a prolonged undervoltage. A **blackout** is a complete power failure. Undervoltages can cause data loss but generally do not cause equipment damage.

An **overvoltage**, or **power surge**, occurs when the incoming electrical power increases significantly above the normal 120 volts. A momentary overvoltage, called a **spike**, occurs when the power increase lasts for less than one millisecond (one thousandth of a second). Uncontrollable disturbances such as lightning bolts cause spikes. Overvoltages can cause immediate and permanent damage to hardware.

To protect against overvoltages and undervoltages, use a surge protector. A **surge protector**, also called a **surge suppressor**, uses special electrical components to smooth out minor noise, provide a stable current flow, and keep an overvoltage from reaching the computer and other electronic equipment (Figure 12-21).



Figure 12-21 Circuits inside a surge protector safeguard against overvoltages and undervoltages.

Resembling a power strip, the computer and other devices plug into the surge protector, which plugs into the power source. The surge protector absorbs small overvoltages — generally without damage to the computer and equipment. Large overvoltages, such as those caused by a lightning strike, often cause the surge protector to fail in order to protect the computer and other equipment.

Surge protectors are not 100 percent effective. Large power surges can bypass the protector. Repeated small overvoltages can weaken a surge protector permanently. Some experts recommend replacing a surge protector every two to three years. Typically, the amount of protection offered by a surge protector is proportional to its cost. That is, the more expensive, the more protection the protector offers.

The surge protector you purchase should meet the safety specification for surge suppression products. This specification, called the **Underwriters Laboratories (UL) 1449 standard**, allows no more than 500 maximum volts to pass through the line. The surge protector also should have a Joule rating of at least 200. A **Joule** is the unit of energy a surge protection device can absorb before it can be damaged. The higher the Joule rating, the better the protection.

If your computer connects to a network or the Internet, be sure also to have protection for your modem, telephone lines, and network lines.

Many surge protectors include plug-ins for telephone lines and other cables. If yours does not, you can purchase separate devices to protect these lines.

For additional electrical protection, many users connect an uninterruptible power supply to the computer. An **uninterruptible power supply (UPS)** is a device that contains surge protection circuits and one or more batteries that can provide power during a temporary or permanent loss of power (Figure 12-22). A UPS connects between your computer and a power source.

Two types of UPS devices are standby and online. A standby UPS, sometimes called an offline UPS, switches to battery power when a problem occurs in the power line. The amount of time a standby UPS allows you to continue working depends on the electrical requirements of the computer and the size of the batteries in the UPS. A UPS for a personal computer should provide from 10 to 30 minutes of use in the case of a total power loss. This should be enough time to save current work and shut down the computer properly.



Figure 12-22 If power fails, an uninterruptible power supply (UPS) uses batteries to provide electricity for a limited amount of time.

An online UPS always runs off the battery, which provides continuous protection. An online UPS is much more expensive than a standby UPS.

Backup Procedures

To prevent against data loss caused by a system failure, computer users should back up files regularly. A **backup** is a duplicate of a file, program, or disk that can be used if the original is lost, damaged, or destroyed. Thus, to **back up** a file means to make a copy of it. In the case of a system failure or the discovery of corrupted files, you **restore** the files by copying the backed up files to their original location on the computer.

You can use just about any media to store backups. Be sure to use high-quality media. Losing data is expensive. High-quality media is worth the investment. A good choice for a home user might be Zip® disks or CD-RWs.

Keep backup copies in a fire-proof and heatproof safe or vault, or offsite. **Offsite** means in a location separate from the computer site. Home and business users utilize offsite storage so that a single disaster, such as a fire, does not destroy both the original and the backup copy of the data. One type of offsite location is a safe deposit box at a bank. A growing trend is to use an Internet hard drive as an offsite location. As discussed in Chapter 7, an Internet hard drive or online storage is a service on the Web that provides storage to computer users.

Business and home users can perform three types of backup: full, differential, or incremental. A **full backup**, sometimes called an **archival backup**, copies all of the files in the computer. A full backup provides the best protection against data loss because it copies all program and data files. Performing a full backup can be time consuming. Users often combine full backups with differential and incremental backups. A **differential backup** copies only the files that have changed since the last full backup. An **incremental backup** copies only the files that have changed since the last full or last incremental backup.

The main difference between a differential backup and an incremental backup is the number of backup files and the time required for backup. With a differential backup, you always have two backups: the full backup and the differential backup that contains all changes since the last full backup.

With incremental backups, you have the full backup and one or more incremental backups. The first incremental backup contains changes since the last full backup. Each incremental backup contains changes only since the previous incremental backup. For files that contain many changes and comprise a large portion of the total data, incremental backup usually is fastest. If files contain only

a few changes, differential backups may be appropriate. Figure 12-23 outlines the advantages and disadvantages of each type of backup.

Backup procedures specify a regular plan of copying and storing important data and program files. Generally, users should perform a full backup at regular intervals, such as at the end of each week and at the end

of the month. Between full backups, you can perform differential or incremental backups. Figure 12-24 shows a sample approach a company might follow for backing up a system for one month. This combination of full and incremental backups provides an efficient way to protect data. Whatever backup procedures a company adopts, they should be stated clearly, documented in writing, and followed consistently.

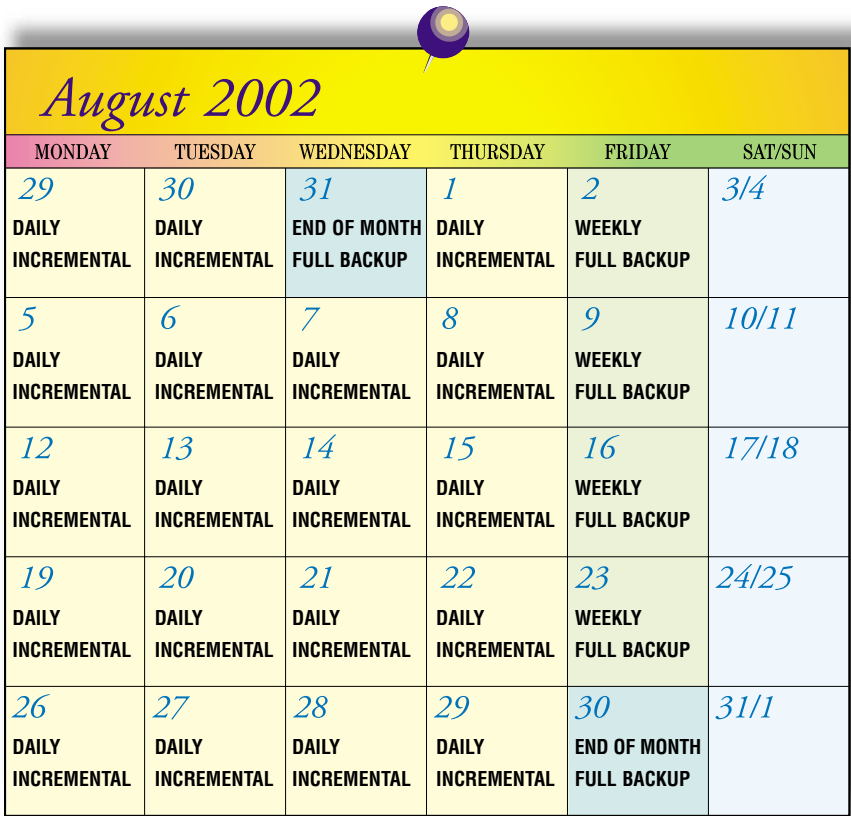


Figure 12-24 This calendar shows a backup strategy for a month. End-of-month backups usually are kept for at least one year.

VARIOUS BACKUP METHODS

TYPE OF BACKUP	ADVANTAGES	DISADVANTAGES
Full	Fastest recovery method. All files are saved.	Longest backup time.
Differential	Fast backup method. Requires minimal space to back up.	Recovery is time consuming because need last full backup plus the differential backup.
Incremental	Fastest backup method. Requires minimal space to back up. Only most recent changes saved.	Recovery is most time consuming because need last full backup and all incremental backups since last full backup.

Figure 12-23 The advantages and disadvantages of various backup methods.

Some users implement a **three-generation backup** policy to preserve three copies of important files. The **grandparent** is the oldest copy of the file. The **parent** is the second oldest copy of the file. The **child** is the most recent copy of the file.

Backup programs are available from many sources. Most operating systems include a backup program. Backup devices, such as tape and removable disk drives, also include backup programs. Numerous stand-alone backup utilities exist. Many of these can be downloaded from the Web at no cost. As discussed in Chapter 8, some vendors offer utility suites that combine several utility programs into a single package or make them available on the Web. These suites typically include a backup utility.

Some companies opt to use an online backup service to handle their backup needs. An **online backup service** is a Web site that automatically backs up your files to their online location. These sites usually charge a monthly or annual fee. If your system crashes, the online backup service typically sends you a CD-ROM that contains all your backed up data. Users with high-speed Internet connections opt for online backup services. For slower connections, these services are not practical.

Disaster Recovery Plan

Every company should develop a disaster recovery plan. A **disaster recovery plan** is a written plan describing the steps a company would take to restore computer operations in the event of a disaster. A disaster recovery plan contains four major components: the emergency plan, the backup plan, the recovery plan, and the test plan.

THE EMERGENCY PLAN An **emergency plan** specifies the steps to be taken immediately after a disaster strikes. The emergency plan usually is organized by type of disaster, such as fire, flood, or earthquake. Depending on the nature and extent of the disaster, emergency procedures will differ. All emergency plans should contain the following information:

1. Names and telephone numbers of people and organizations to notify (e.g., management, fire department, police department)
2. Procedures to follow with the computer equipment (e.g., equipment shutdown, power shutoff, file removal)
3. Employee evacuation procedures
4. Return procedures; that is, who can re-enter the facility and what actions they are to perform

THE BACKUP PLAN Once the procedures in the emergency plan have been executed, the next step is to follow the backup plan. The **backup plan** specifies how a company uses backup files and equipment to resume information processing. The backup plan should specify the location of an alternate computer facility in the event the company's normal location is destroyed or unusable. The backup plan identifies these items:

1. The location of backup data, supplies, and equipment
2. The personnel responsible for gathering backup resources and transporting them to the alternate computer facility
3. A schedule indicating the order and approximate time each application should be up and running

For a backup plan to be successful, it is crucial the company backs up all critical resources. It also is crucial that additional people, including possibly non-employees, are trained in the backup and recovery procedures because company personnel could be injured in a disaster.

The location of the alternate computer facility is important. It should be close enough to be convenient, yet not too close that a single disaster, such as an earthquake, could destroy both the main and alternate computer facilities. Some companies pre-install all the necessary hardware, software, and communications devices at the alternate computer facility. These facilities immediately are ready in the event of a disaster. In other cases, the alternate computer facility is simply an empty facility that can accommodate the necessary computer resources, if necessary. Another alternative is to enter into a **reciprocal backup relationship** with another firm, where one firm provides space and sometimes equipment to the other in case of a disaster.

THE RECOVERY PLAN The **recovery plan** specifies the actions to be taken to restore full information processing operations. As with the emergency plan, the recovery plan differs for each type of disaster. To prepare for disaster recovery, a company should establish planning committees, with each one responsible for different forms of recovery. For example, one committee is in charge of hardware replacement. Another is responsible for software replacement.

THE TEST PLAN To provide assurance that the disaster plan is complete, it should be tested. A disaster recovery **test plan** contains information for simulating various levels of disasters and recording an organization's ability to recover. In a simulation, all personnel follow the steps in the disaster recovery plan. Any needed recovery actions that are not specified in the plan should be added. Although simulations can be scheduled, the best test of the plan is to simulate a disaster without advance notice.

Developing a Computer Security Plan

A company should incorporate the individual risks and safeguards previously mentioned and the disaster recovery into an overall computer security plan. A **computer security plan** summarizes in writing all of the safeguards that are in place to protect a company's information assets. A computer security plan should do the following:

1. Identify all information assets of an organization, including hardware, software, documentation, procedures, people, data, facilities, and supplies.
2. Identify all security risks that may cause an information asset loss. Rank risks from most likely to occur to least likely to occur. Place an estimated value on each risk, including the value of lost business. For example, what is the estimated loss if customers cannot place orders for one hour, one day, or one week?
3. For each risk, identify the safeguards that exist to detect, prevent, and recover from a loss.

Web Link

For more information on the International Computer Security Association, visit the Discovering Computers 2002 Chapter 12 WEB LINK page (scs.site.com/dc2002/ch12/weblink.htm) and click International Computer Security Association.

The company should evaluate the computer security plan annually or more frequently for major changes in information assets, such as the addition of a new computer or the implementation of a new application. In developing the plan, keep in mind that some degree of risk is unavoidable. The more secure a system is, the more difficult it is for everyone to use. The goal of a computer security plan is to match an appropriate level of safeguards against the identified risks. Fortunately, most organizations will never experience a major information system disaster.

Companies and individuals who need help with computer security plans can contact the **International Computer Security Association (ICSA)** via the telephone or on the Web for assistance (Figure 12-25).

INTERNET AND NETWORK SECURITY

Information transmitted over networks has a higher degree of security risk than information kept on a company's premises. The Internet and networks employ many security techniques discussed thus far such as user names, passwords, biometrics, and callback systems. Network administrators usually take measures to protect a network from security risks. On a vast network such as the Internet with no central administrator, the risk is even greater. Every computer along the path of your data can see what you send and receive. Fortunately, most Web browsers and many Web sites use techniques to keep data secure and private.

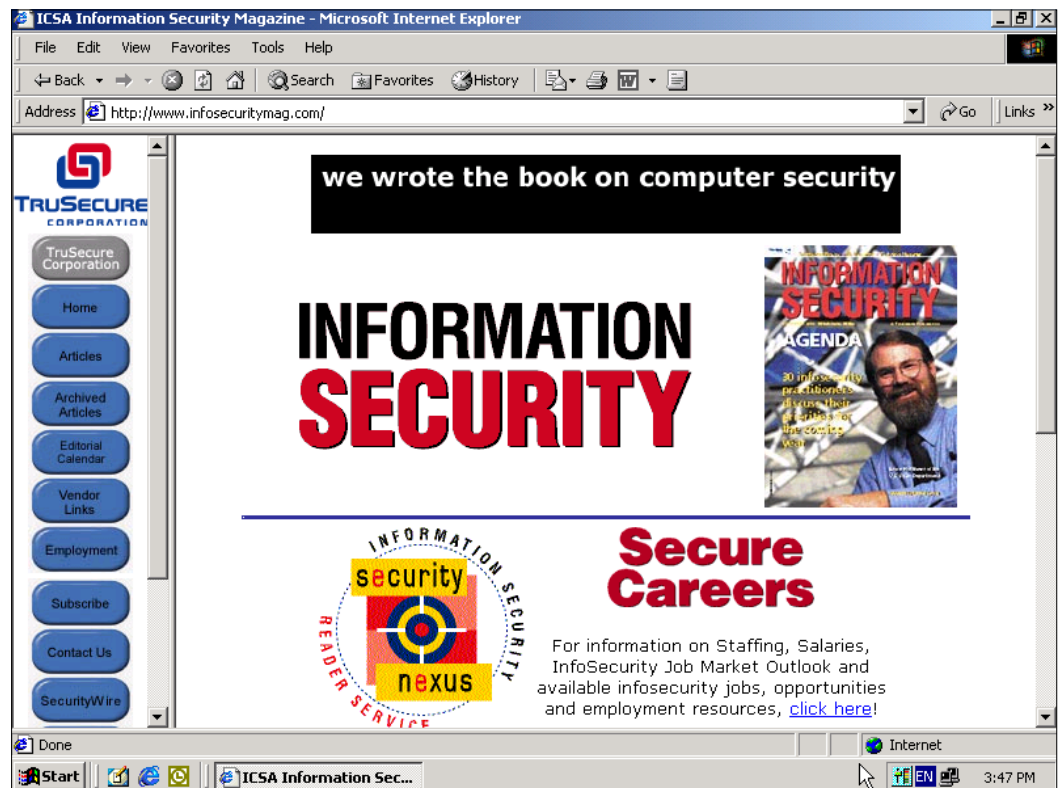


Figure 12-25 The ICSA is available for companies or individuals that need assistance with computer security plans.

The following pages address the increased risks associated with networks and the measures you can take to protect your systems while online. Most businesses use more than one of these security techniques.

Securing Internet Transactions

To provide secure data transmission, many Web browsers use encryption. Newer versions of Netscape Navigator and Microsoft Internet Explorer use RSA. Recall that RSA is a very popular public key encryption technology. Some browsers offer a protection level known as 40-bit encryption. Many offer 128-bit encryption, which is an even higher level of protection. Applications requiring more security, such as banks, brokerage firms, or online retailers that use credit card or other financial information, use 128-bit encryption.

A Web site that uses encryption techniques to secure its data is known as a **secure site**. Secure sites use

digital certificates along with a security protocol. Two popular security protocols are Secure Sockets Layer and Secure HTTP. Credit card transactions sometimes use the Secure Electronics Transaction specification. The following paragraphs discuss each of these encryption techniques.

DIGITAL CERTIFICATES A **digital certificate**, also called a **public-key certificate**, is a notice that guarantees a user or a Web site is legitimate. E-commerce applications commonly use digital certificates.

A **certificate authority (CA)** or **issuing authority (IA)** is an authorized company or person that issues and verifies digital certificates. You apply for a digital certificate from a CA (Figure 12-26). A digital certificate typically contains your name, your public key and its expiration date, the issuing CA's name and signature, and the serial number of the certificate. The information in a digital certificate is encrypted using the CA's private key.

Web Link

For more information on digital certificates, visit the Discovering Computers 2002 Chapter 12 WEB LINK page (scs.site.com/dc2002/ch12/weblink.htm) and click Digital Certificates.

COMPANY ON THE CUTTING EDGE

SYMANTEC.

Internet Security

You lock the door to your apartment and exercise extra caution when walking alone at night. But do you protect your computer from hacker attacks or theft of your personal and financial data? Probably not, according to a survey conducted by Applied Marketing Research, Inc. Only about one in five personal computer users has some sort of personal firewall to deter cybercriminals.

Although nearly 90 percent of these users have installed an antivirus program, they are leaving their computers open to attack each time they surf the Internet or buy products online.

Symantec is one of the world's premier Internet security technology companies with operations in more than 33 countries. Its more than 2,600 employees develop mobile code protection and e-mail and Internet content filtering programs, along with antivirus and risk management software to protect 60 million users against malicious threats. Ninety-eight of the Fortune 100 companies use one or more of these products daily.

For more information on Symantec, visit the Discovering Computers 2002 Companies Web page (scs.site.com/dc2002/companies.htm) and click Symantec.



Figure 12-26 VeriSign is a certificate authority that issues and verifies digital certificates.

SECURE SOCKETS LAYER **Secure Sockets Layer (SSL)** provides private-key encryption of all data that passes between a client and a server. SSL requires the client has a digital certificate. Once the server has a digital certificate, the Web browser communicates securely with the client. Web pages that use SSL typically begin with https, instead of http (Figure 12-27).

SECURE HTTP **Secure HTTP (S-HTTP)** allows you to choose an encryption scheme for data that passes between a client and a server. With S-HTTP, the client and server both must have digital certificates. S-HTTP is more difficult to use than SSL, but it is more secure. Applications that must verify the authenticity of a client, such as for online banking, use S-HTTP.

SECURE ELECTRONIC TRANSACTION The **Secure Electronic Transaction (SET)** specification uses a public-key encryption to secure credit-card transaction systems. The SET specification is quite complex, making it slow on some systems.

Securing E-mail Messages

When you send an e-mail message over the Internet, just about anyone can read it. If you are sending personal or confidential information in the message, you should protect the message from prying eyes. An unprotected e-mail sent through the Internet is similar to sending a postcard through the United States mail. Two ways to protect an e-mail message are to encrypt it and to sign it digitally.

One of the most popular e-mail encryption programs is **Pretty Good Privacy (PGP)**. PGP is freeware for personal, non-commercial users. Home users can download PGP from the Web at no cost. PGP uses a public-key encryption scheme. As shown in

Figure 12-20 on page 12.17, when you receive an e-mail message encrypted with your public key, you use your private key to decrypt the message.

A **digital signature**, also called a **digital ID**, is an encrypted code that a person, Web site, or company attaches to an electronic message to verify the identity of the message sender. The code usually consists of the user's name and a hash of all or part of the message. A **hash** is a mathematical formula that generates a code from the contents of the message. Thus, the hash differs for each message.

Digital signatures use a public key method. Senders use their private key to encrypt their digital signature. Receivers of the message use the sender's public key to decrypt the digital signature. The recipient then generates a new hash of the received message and compares it to one in the digital signature to ensure they match.

Digital signatures often are used to ensure that an impostor is not participating in an Internet transaction. That is, digital signatures help to prevent e-mail forgery. A digital signature also can verify that the content of a message has not changed.

Firewalls

Despite efforts to protect the data on your computer's hard disk, it still is vulnerable to attacks from a hacker. A **firewall** is a security system consisting of hardware and/or software that prevents unauthorized access to data and information on a network. Companies use firewalls to deny network access to outsiders and to restrict employees' access to sensitive data such as payroll or personnel records.

To implement a firewall, many large companies route all communications through a proxy

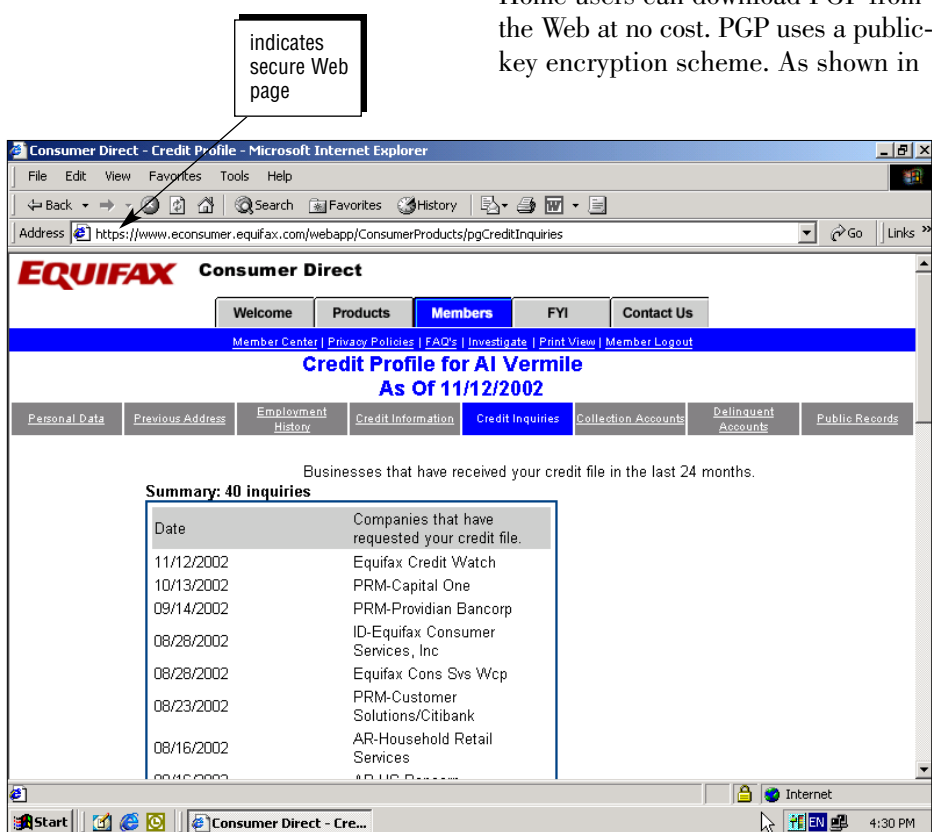


Figure 12-27 Secure Web pages often begin with https instead of http.

server. A **proxy server** is a server outside the company's network that controls which communications pass into the company's network. That is, the firewall carefully screens all incoming and outgoing messages.

Firewalls use a variety of screening techniques. Some check the domain name or IP address of the message for legitimacy. Others require the messages have digital signatures.

All networked or online computer users should have a firewall. Businesses can implement a firewall solution themselves or outsource their needs to a company that specializes in providing firewall protection. Home and small office/home office users should install personal firewalls.

A **personal firewall** is a software program that detects and protects your personal computer and its data from unauthorized intrusions. These products constantly monitor all transmissions to and from your computer and inform you of any attempted intrusion (Figure 12-28). These easy-to-use products are definitely worth their expense, which usually is less than \$50. The table in Figure 12-29 lists popular personal firewall products.

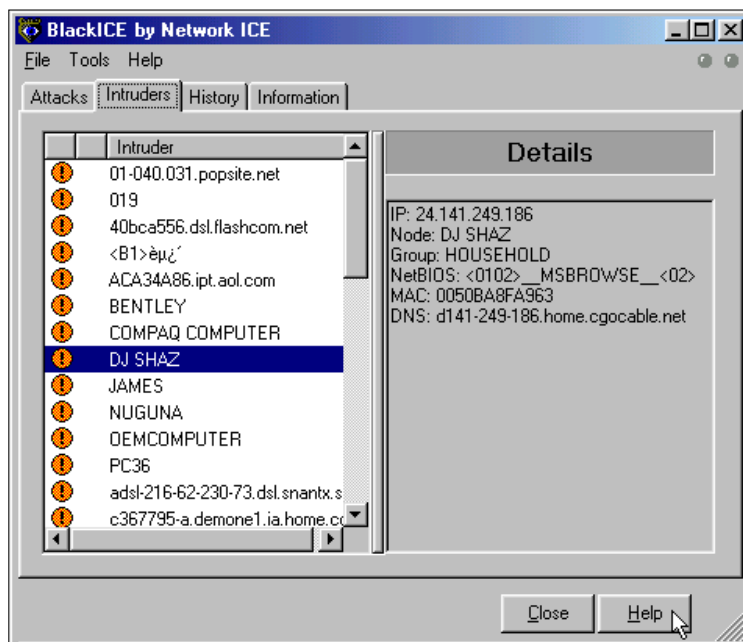


Figure 12-28 Personal firewall packages detect and protect your personal computer from hackers.



When you think about a firewall, you might think about a business network. Firewalls keep out hackers and others who attempt to steal data or crash your system. Traditionally, firewall software for the home user was too expensive, difficult to install, and rarely needed when most individuals used slow dial-up modems. Enter broadband access and personal computers with new high-speed always on DSL or cable modem connections and the personal firewall moves into the mainstream. Today, a variety of inexpensive and even almost free shareware programs exists for the home user. This new class of host-based firewalls typically protects a single personal computer against network threats. These programs are easy to use and easy to install.

If you have a home network connecting several computers that share a broadband link to the Internet, you should consider installing a network firewall. Unlike a personal firewall, which usually is software only, a network firewall often is a combination of software and hardware that creates a secure barrier between your network and the Internet.

You probably would benefit from a home network or personal firewall if your computing practices include any of the following:

- Your computer files need to be accessed remotely across the network
- You use any sort of Internet-based remote control or remote access program such as PC Anywhere, Laplink, or Wingate
- You want to monitor your Internet connection for intrusion attempts
- You operate an Internet server such as Personal Web Server
- You want to protect your system from Trojan horse virus programs

For more information on personal firewalls and home network firewalls, visit the Discovering Computers 2002 Apply It Web page (scsite.com/dc2002/apply.htm) and click Chapter 12 Apply It #2.

POPULAR PERSONAL FIREWALL PRODUCTS

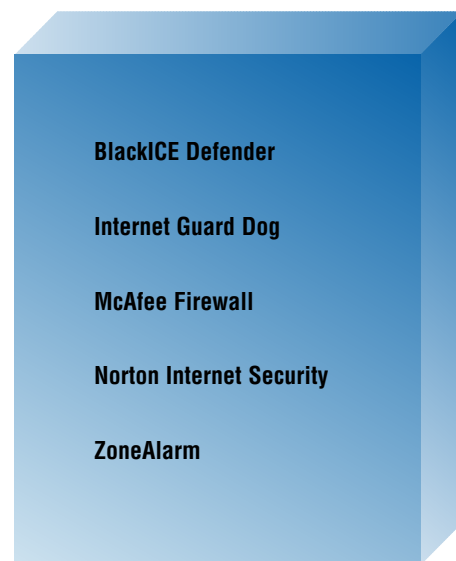


Figure 12-29 Popular personal firewall products.

Web Link

For more information on online security services, visit the Discovering Computers 2002 Chapter 12 WEB LINK page (scsite.com/dc2002/ch12/weblink.htm) and click Online Security Services.

TECHNOLOGY TRAILBLAZER**DONN PARKER**

Computer crime cannot be predicted, according to the Parker Philosophy. Consequently, companies cannot prepare for future threats based on previous attacks. Donn Parker ought to know — he is one of the world's leading authorities on cybercrime.

For the past 30 years, Parker has been interviewing more than 200 computer criminals and reviewing thousands of cases of reported security crimes. He has learned that these crooks are unpredictable and irrational. They generally believe they are acting ethically and that violating the law is the best method of solving deep personal problems.

Companies can fight cybercrime by using Parker's Peer Principle: Share information about the vulnerability of attacks, develop security methods, and then apply and practice these models.

With six books published on computer security, Parker has participated in more than 250 security reviews for major corporations. His most recent book is *Fight Computer Crime, a New Frame for Protecting Information*. He has appeared on *60 Minutes*, *20/20*, and *NOVA* and has been featured in *People* and the *Los Angeles Times*. He earned bachelor's and master's degrees from the University of California at Berkeley.

For more information on Donn Parker, visit the Discovering Computers 2002 People Web page (scsite.com/dc2002/people.htm) and click Donn Parker.



To further protect your personal computer from unauthorized intrusions, you should disable File and Print Sharing on your Internet connection (Figure 12-30). This security measure attempts to ensure that others cannot access your files or your printer.

To determine if your computer is vulnerable to a hacker attack, you could use an online security service. An **online security service** is a Web site that evaluates your computer to check for Web and e-mail vulnerabilities. The service then provides recommendations of how to deal with the vulnerabilities.

INFORMATION PRIVACY

Information privacy refers to the right of individuals and companies to deny or restrict the collection and use of information about them. In the past, information privacy was easier to maintain because information was kept in separate locations. Retail stores each had their own credit files. Each government agency maintained separate records. Doctors had their own patient files.

Today, huge databases store this data in online databases. Much of the data is personal and confidential and

should be accessible to only authorized users. Many individuals and organizations, however, question whether this data really is private. That is, some companies and individuals collect and use this information without your authorization. Many Web sites collect data about you so they can customize advertisements and send you personalized e-mail messages. Some employers monitor your computer usage and e-mail messages.

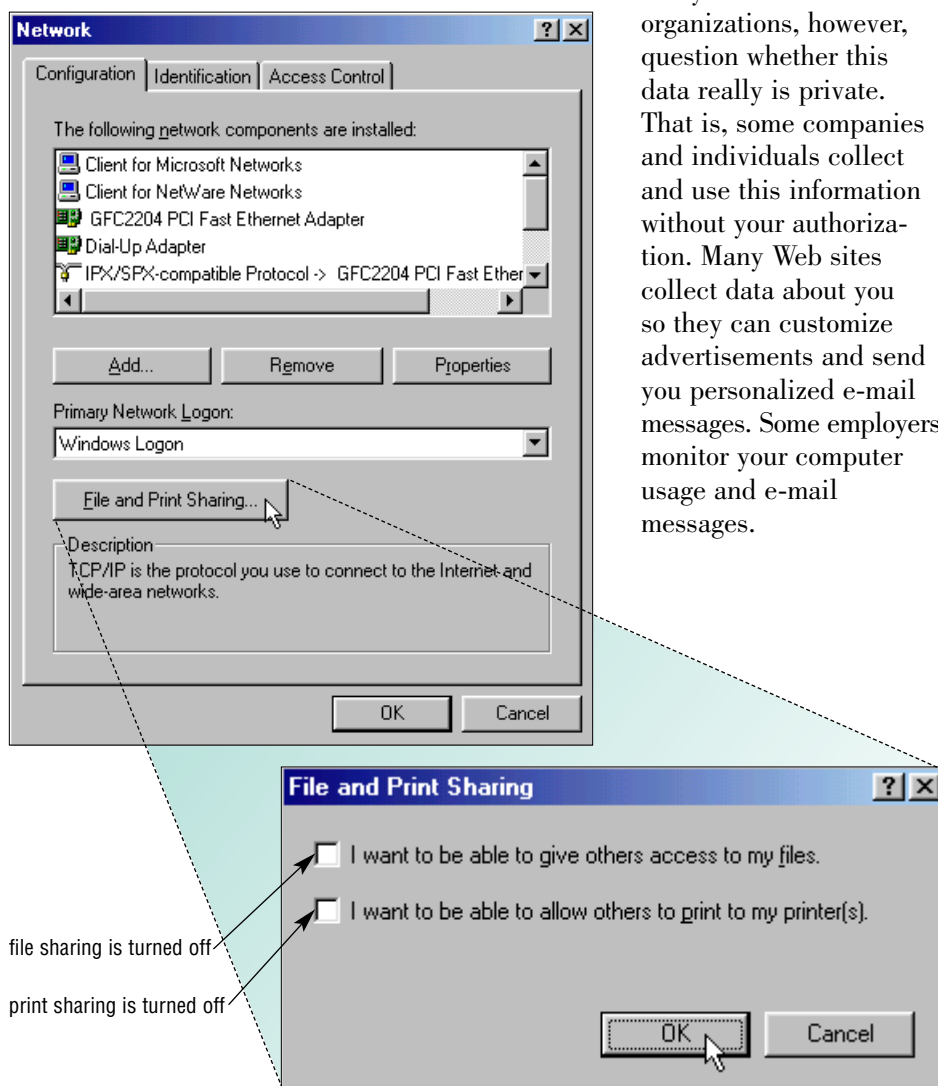


Figure 12-30 To protect files on your local hard disk from hackers, turn off File and Print Sharing on your Internet connection.

The following sections address techniques companies and employers use to collect your personal data. Figure 12-31 lists actions you can take to make your personal data more private.

Electronic Profiles

When you fill out a form such as a magazine subscription, product warranty registration card, or contest entry form, the merchant that receives

the form usually enters it into a database. Likewise, every time you click an advertisement on the Web or register a software product online, your information and preferences enter a database. Merchants then sell the contents of their databases to national marketing firms and Internet advertising firms. By combining this data with information from public sources such as driver's license and vehicle registrations, these firms create an electronic profile of individuals.

The marketing and advertising firms pride themselves on being able to collect accurate, in depth information about people. The information in an electronic profile includes very personal details such as your age, address, telephone number, spending habits, marital status, number of dependents, ages of dependents, and so on.

These firms then sell your electronic profile to any company that requests it. A car dealership may

How to Safeguard Personal Information

1. Fill in only necessary information on rebate, warranty, and registration forms.
2. Do not preprint your telephone number or Social Security number on personal checks.
3. Have an unlisted or unpublished telephone number.
4. If Caller ID is available in your area, find out how to block your number from displaying on the receiver's system.
5. Do not write your telephone number on charge or credit receipts.
6. Ask merchants to not write credit card numbers, telephone numbers, Social Security numbers, and driver's license numbers on the back of your personal checks.
7. Purchase goods with cash, rather than credit or checks.
8. Avoid shopping clubs and buyers' cards.
9. If a merchant asks personal questions, find out why they want to know before releasing the information.
10. Inform merchants that you do not want them to distribute your personal information.
11. Ask, in writing, to be removed from mailing lists.
12. Obtain your credit report once a year from each of the three major credit reporting agencies (Equifax, Experian, and TransUnion) and correct any errors.
13. Request a free copy of your medical records once a year from the Medical Information Bureau.
14. Limit the amount of information you provide to Web sites. Just fill in required information.
15. Install a cookie manager to filter cookies.
16. Clear your history file when you are finished browsing.
17. Set up a free e-mail account. Use this e-mail address for merchant forms.
18. Turn off File and Print Sharing on your Internet connection.
19. Install a personal firewall.
20. Sign-up for e-mail filtering through your Internet service provider or use an anti-spam program such as Brightmail.
21. Do not reply to spam for any reason.
22. Surf the Web anonymously with programs such as Freedom or through an anonymous Web site such as Anonymizer.

Figure 12-31 Techniques to keep personal data private.

Web Link

For more information on cookies, visit the Discovering Computers 2002 Chapter 12 WEB LINK page (scs.site.com/dc2002/ch12/weblink.htm) and click Cookies.

ISSUE**Personal Information for Sale****Privacy Invasion**

The State of Virginia has a law that declares that "Any person whose name, portrait, or picture is used without having first obtained the written consent of such person ... for advertising purposes or for the purposes of trade, such persons may maintain a suit in equity against the person, firm..." Citing this law, a Virginia resident recently filed a claim against a national magazine challenging the right of the magazine to sell or rent his name and other personal information to another publication without his express written consent. The company obtained the personal information when the Virginia resident filled out an online registration form to obtain a free sample copy of a magazine. When you fill out online forms or purchase an item online, the retailer has your e-mail address and other personal information. Should these retailers be allowed to send you marketing pieces? Should they be allowed to sell your e-mail address to others? Is this an ethical practice? Should there be a Federal law prohibiting companies from selling your personal information? Why or why not?

For more information on personal information and privacy issues, visit the Discovering Computers 2002 Issues Web page (scs.site.com/dc2002/issues.htm) and click Chapter 12 Issue #2.

want to send an advertisement piece or e-mail message to all sports car owners in its vicinity. Thus, the dealership may request a list of all sports car owners living in the southeastern United States.

Direct marketing supporters say that using information in this way lowers overall selling costs, which lowers product prices. Critics contend that the information in an electronic profile can reveal more about an individual than anyone has a right to know. They claim that companies should inform people if they plan to provide personal information to others. Further, people should have the right to deny such use. Many companies today allow you to specify whether you want them to distribute your personal information (Figure 12-32).

Cookies

Webcasting, e-commerce, and other Web applications often rely on cookies to identify users and customize Web pages. A **cookie** is a small file that a Web server stores on *your* computer. Cookie files typically contain data about you, such as your user name or viewing preferences. Many commercial Web sites send a cookie to your browser, and then your computer's hard disk stores the cookie. The next time you visit the Web site, your browser retrieves the cookie from your hard disk and sends the data in the cookie to the Web site. Web sites use cookies for a variety of purposes.

Figure 12-32 Many companies today allow you to specify whether you want them to distribute your personal information.

- Web sites that allow for personalization often use cookies to track user preferences (Figure 12-33). On such sites, you may be asked to fill in a form requesting personal information, such as your name, zip code, or site preferences. A news site, for example, might allow you to customize your viewing preferences to display certain stock quotes. The site stores your preferences in a cookie on your hard disk.
- Some Web sites use cookies to store your password so that you do not need to enter it every time you log in to their site.
- Online shopping sites generally use a **session cookie** to keep track of items in your shopping cart. This way, you can start an order during one Web session and finish it on another day in another session. Session cookies usually expire after a certain time period, such as a week or a month.
- Some Web sites use cookies to track how regularly you visit a site and the Web pages you visit while at the site.
- Web sites may use cookies to target advertisements. These sites store your interests and browsing habits in the cookie.

A Web site can read data only from its own cookie file. It cannot access or view any other data on your hard disk — including another cookie file. Some Web sites do sell or trade information stored in your cookie to advertisers — a practice many believe to be unethical. If you do not want your personal information to be distributed, you should limit the amount of information you provide to a Web site.

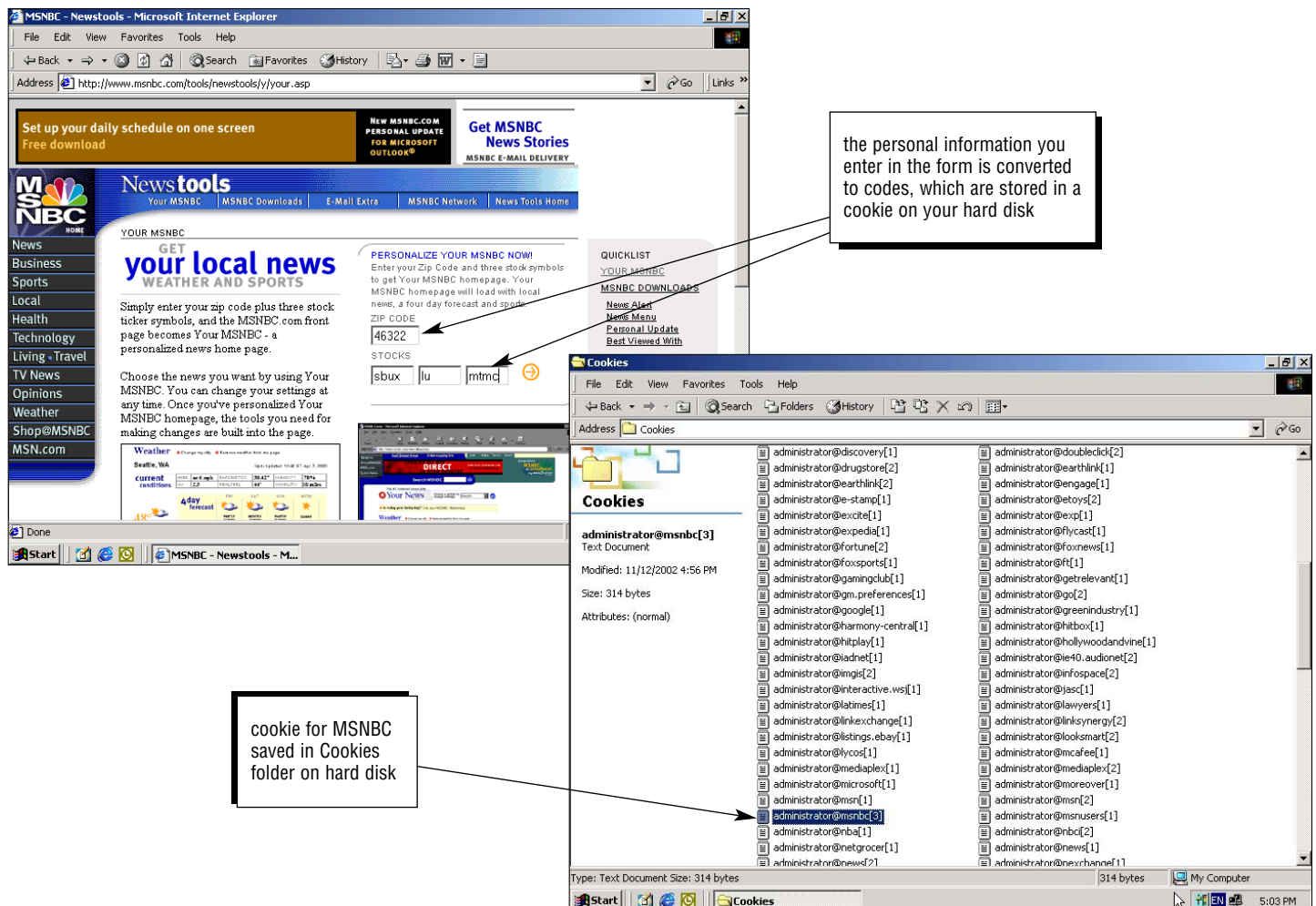


Figure 12-33 Some Web sites store user preferences in a cookie on your hard disk.



Cookie Anyone?

Web Server Cookies – Do They Threaten Your Privacy?

Cookies are small files that online companies transfer to your computer's hard disk through your Web browser. These files enable a company's system to track your online activities. Examples of information that a cookie can collect from a user includes the computer's IP address; login name and password; e-mail address; the computer's operating system and platform; the type of and version number of the user's browser; the date, time, and length of time the host system was accessed; and the pages visited while the user was online. Many consumer groups and privacy advocates are taking legal action because of this collection of information. They contend that companies are not doing enough to protect the privacy of Web users. As a result of several of these class-action lawsuits, the giant online retailer Amazon.com (see URL below) has revamped its privacy policy. An overview of the new policy is contained on their Web site and explains what information the company gathers, why it gathers that information, and by what means it gathers that information. Do you think that all online companies should be required to post their policies and explain what information they collect and how it is used? Should this be enforced by the Federal government? Should you, as a private citizen, have the right to sue companies who collect this information for privacy invasion? Why or why not?

For more information on cookies and privacy issues and the Web site mentioned above, visit the Discovering Computers 2002 Issues Web page (scs.site.com/dc2002/issues.htm) and click Chapter 12 Issue #3.

You can set your browser to accept cookies automatically, prompt you if you wish to accept a cookie, or disable cookie use altogether (Figure 12-34). Keep in mind if you disable cookie use, you will not be able to use

many of the e-commerce Web sites. As an alternative, you can purchase a software program that selectively blocks cookies. Figure 12-35 outlines these and other types of cookie managers.

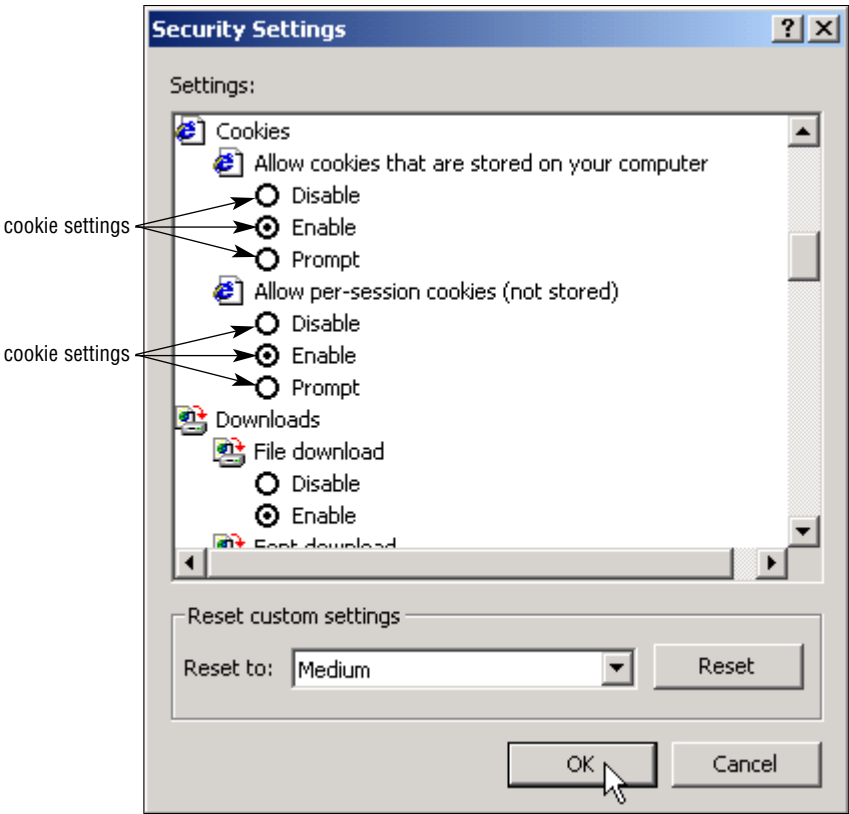


Figure 12-34 You can change cookie settings through Windows.

COOKIE MANAGERS

Program Name	Function
AdSubtract SE	Block advertising and cookies
Cookie Cruncher	View, edit, and delete cookies
Cookie Crusher	Accept or reject cookies by Web site – tells you purpose of cookie (tracking, shopping cart, etc.)
IEClean, NSClean	Delete cookies; also can delete cache, history files, and other browsing files
Internet Junkbuster Proxy	Advertising and cookie blocker that allows you to block or allow cookies based on their domain name
WebWasher	Blocks advertising banners and associated cookies
Window Washer	Delete cache, history, and cookie files

Figure 12-35 Popular cookie manager programs.

Spyware

Spyware is a program placed on a computer without the user's knowledge that secretly collects information about the user. Spyware can enter your computer as a virus or as a result of installing a new program. The spyware program communicates information it collects to some outside source while you are online.

Some Internet advertising firms use spyware, which in this case is called **adware**, to collect information about user's Web browsing habits. (Cookies are not considered spyware because you know they exist; otherwise they operate in a manner similar to spyware.)

If you download software from the Web, pay careful attention to the license agreement and registration information requested during installation. The software provider, in principle, should notify you that your information may be communicated to advertisers. To remove spyware, you need to purchase a special program that can detect and delete it.

Spam

Spam is an unsolicited e-mail message or newsgroup posting sent to many recipients or newsgroups at once. Spam is Internet junk mail (Figure 12-36). The content of spam ranges from selling a product or service, to

promoting a business opportunity, to advertising offensive material.

You can reduce the amount of spam you receive by signing up for e-mail filtering from your Internet service provider. **E-mail filtering** is a service that blocks e-mail messages from designated sources. These services typically collect the spam in a central location that you can view at any time. An alternative to e-mail filtering is to purchase an **anti-spam program** that attempts to remove spam. Sometimes, though, these programs remove valid e-mail messages.

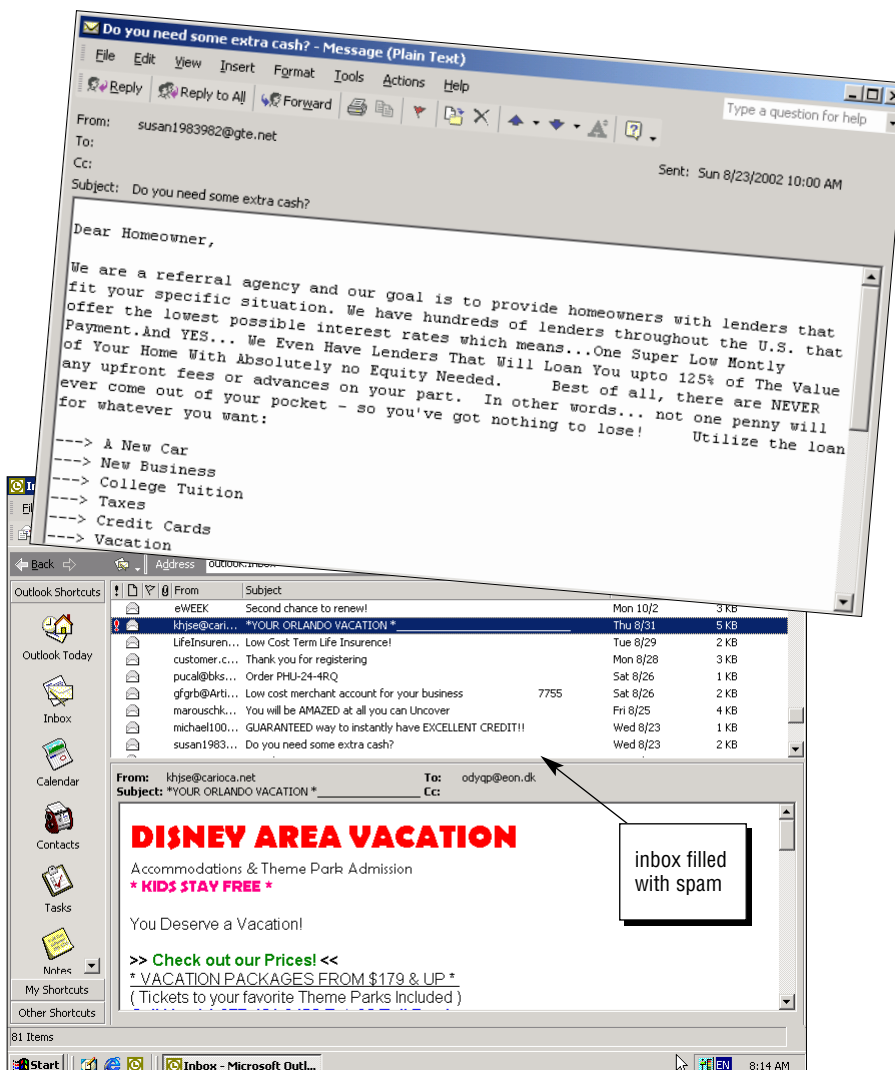


Figure 12-36 Spam is Internet junk mail.

ISSUE

Cybersleuths to the Rescue

Catching Unauthorized Intruders

Companies do not like to publicize breaches to their security systems. A recent survey, however, uncovered that more than 60 percent of organizations have fallen victim to cybercrime. Online intruders range from curiosity seekers to pranksters to criminals to terrorists. Their crimes range from accessing and erasing confidential records, to causing airport computers to malfunction, to paralyzing a hospital information system, to attaching a virus to an e-mail message and sending it across the Internet. In response to these cybercrimes, a new type of detective, called a cybersleuth, has emerged. Instead of footprints, cybersleuths use clues on hard disks to solve a cybercrime. Fighting computer crime is challenging because it is a relatively new phenomenon. Cybersleuths cannot use the proven crime-fighting techniques that have been used for centuries to solve other non-computer crimes. What skills and abilities do you think a cybersleuth must possess? Why? Would you be a good cybersleuth? Why or why not?

For more information on cybercrime and cybersleuths, visit the Discovering Computers 2002 Issues Web page (scs.site.com/dc2002/issues.htm) and click Chapter 12 Issue #4.

Privacy Laws

The concern about privacy has led to federal and state laws regarding the storage and disclosure of personal data (Figure 12-37). Common points in some of these laws include the following:

1. Information collected and stored about individuals should be limited to what is necessary to carry out the function of the business or government agency collecting the data.
2. Once collected, provisions should be made to restrict access to the data to those employees within the organization who need access to it to perform their job duties.
3. Personal information should be released outside the organization collecting the data only when the person has agreed to its disclosure.
4. When information is collected about an individual, the individual should know that the data is being collected and have the opportunity to determine the accuracy of the data.

Several federal laws deal specifically with computers. The 1986 **Electronic Communications Privacy Act (ECPA)** provides the same protection that covers mail and telephone communications to electronic communications such as voice mail. The 1988 **Computer Matching and Privacy Protection Act** regulates the use of government data to determine the eligibility of individuals for federal benefits. The 1984 and 1994 **Computer Fraud and Abuse Acts** outlaw unauthorized

DATE	LAW	PURPOSE
1998	Child Online Protection Act (COPA)	Penalizes online commercial entities that knowingly distribute material deemed harmful to minors.
1997	No Electronic Theft (NET) Act	Closed a narrow loophole in the law that allowed people to give away copyrighted material (such as software) on the Internet without legal repercussions.
1996	National Information Infrastructure Protection Act	Penalizes theft of information across state lines, threats against networks, and computer system trespassing.
1994	Computer Abuse Amendments Act	Amends 1984 act to outlaw transmission of harmful computer code such as viruses.
1992	Cable Act	Extends privacy of Cable Communications Policy Act of 1984 to include cellular and other wireless services.
1991	Telephone Consumer Protection Act	Restricts activities of telemarketers.
1988	Computer Matching and Privacy Protection Act	Regulates the use of government data to determine the eligibility of individuals for federal benefits.
1988	Video Privacy Protection Act	Forbids retailers from releasing or selling video-rental records without customer consent or a court order.
1986	Electronic Communications Privacy Act (ECPA)	Provides the same right of privacy protection for the postal delivery service and telephone companies to the new forms of electronic communications, such as voice mail, e-mail, and cellular telephones.
1984	Cable Communications Policy Act	Regulates disclosure of cable television subscriber records.
1984	Computer Fraud and Abuse Act	Outlaws unauthorized access of federal government computers.
1978	Right to Financial Privacy Act	Strictly outlines procedures federal agencies must follow when looking at customer records in banks.
1974	Privacy Act	Forbids federal agencies from allowing information to be used for a reason other than for which it was collected.
1974	Family Educational Rights and Privacy Act	Gives students and parents access to school records and limits disclosure of records to unauthorized parties.
1970	Fair Credit Reporting Act	Prohibits credit reporting agencies from releasing credit information to unauthorized people and allows consumers to review their own credit records.

Figure 12-37 Summary of the major U.S. government laws concerning privacy.

access to federal government computers and the transmission of harmful computer code such as viruses.

One law with an apparent legal loophole is in the 1970 **Fair Credit Reporting Act**. The act limits the rights of others viewing a credit report to those with a legitimate business need. The problem is that it does not define a legitimate business need. The result is that just about anyone can say they have a legitimate business need and gain access to your credit report.

Credit reports contain much more than just balance and payment information on mortgages and credit cards. The largest credit bureaus maintain information on family income, number of dependents, employment history, bank balances, driving records, lawsuits, and Social Security numbers. In total, these credit bureaus have more than 400 million records on more than 160 million people. Some credit bureaus sell combinations of the data they have in their databases to direct marketing organizations. The U.S. Congress is considering a major revision of the Fair Credit Reporting Act because of continuing complaints about credit report errors and the invasion of privacy.

Employee Monitoring

Employee monitoring involves the use of computers to observe, record, and review an individual's use of a computer, including communications such as e-mail, keyboard activity (used to measure productivity), and Web sites visited. Many software programs exist that easily allow employers to monitor employees. Further, it is legal for employers to use these software programs.

A frequently debated issue is whether an employer has the right to read employee e-mail messages. Actual policies vary widely. Some companies declare that they will review e-mail messages regularly and others state that e-mail is private. If a company does not have a formal e-mail policy, it can read e-mail without employee notification. One survey discovered that more than 73 percent of companies search and/or read

employee files, voice mail, e-mail, Web connections, and other networked communications. Another claimed that 25 percent of companies have fired employees for misusing communications technology.

At present, no laws exist relating to e-mail. The 1986 Electronic Communications Privacy Act does not cover communications within a company because any piece of mail sent from an employer's computer is considered company property. Several lawsuits have been filed against employers because many believe that such internal communications should be private. In response to the issue of workplace privacy, the U.S. Congress proposed the **Privacy for Consumers and Workers Act**, which states that employers must notify employees if they are monitoring electronic communications. Supporters of the legislation hope that it also will restrict the types and amount of monitoring that employers can conduct legally.



How Private Is Your Credit Report?

Information Privacy

Your credit report is a gold mine of information. It contains your Social Security number, home address, employment data, credit history, payment status, and even legal information. Federal and state laws restrict who has access to this sensitive information and what uses can be made of it. Anyone with a legitimate business need, however, can gain access to your credit report. In some states, companies known as information vendors can obtain and resell credit reports. Alternatively, credit bureaus frequently provide lists of individuals who meet certain credit criteria to companies that offer pre-approved credit cards or other lines of credit. Can information collected by a credit bureau present a privacy threat? How carefully should credit bureaus be required to monitor the requests for your credit report? Should credit bureaus be able to sell your report to information vendors? Should Federal law require that they first have your permission before they distribute your credit history?

For more information on privacy and credit reports, visit the Discovering Computers 2002 Issues Web page (scsite.com/dc2002/issues.htm) and click Chapter 12 Issue #5.

ISSUE

Freedom Challenge?

Web Filtering and Censorship

An issue heavily debated in the United States and around the world is Internet censorship. In many states and within the Federal government, politicians are attempting to pass laws and legislation that would permit the government and other agencies to regulate Internet content. The public libraries and schools are the main focus of many of these proposed laws. In general, these laws would require that these public institutions use filtering software. This type of software prevents users from accessing a wide range of information, including such topics as art, literature, politics, religion, and free speech. The American Civil Liberties Union (see URL below) and other similar organizations vehemently oppose any type of legislative censorship. Instead, they argue, it is the responsibility of the parent to control what content their child accesses at a library. They suggest that schools have acceptable use policies and that the schools be responsible for enforcing those policies. They further contend that without free and unregulated access to the Internet, this exciting new medium could become, for many Americans, little more than a G-rated television network. Do you agree or disagree that the government should control Internet content? Is control even possible? Should a college or university use filtering software? Should college students be able to use school computers to access any Web site of their choice or should the school use filtering software?

For more information on censorship and filtering software and the Web site mentioned above, visit the Discovering Computers 2002 Issues Web page (scs.site.com/dc2002/issues.htm) and click Chapter 12 Issue #6.

Protecting Children from Objectionable Material

One of the most controversial issues surrounding the Internet is the availability of objectionable material, such as racist literature and obscene pictures. Some believe that such materials should be banned. Others believe that the materials should be filtered; that is, restricted and unavailable to minors. Internet filtering opponents argue that banning any materials violates constitutional guarantees of free speech and personal rights.

Responding to pressure for restrictions, in February 1996, President Clinton signed the **Communications Decency Act**, which made it a criminal offense to distribute indecent or patently offensive material online. In June 1997, the Supreme Court declared the law unconstitutional because it violated the guarantee of free speech.

One approach to restricting access to certain material is a rating system similar to those used for movies and videos (Figure 12-38). If content at the Web site goes beyond the rating limits set in the Web browser software, a user cannot access the

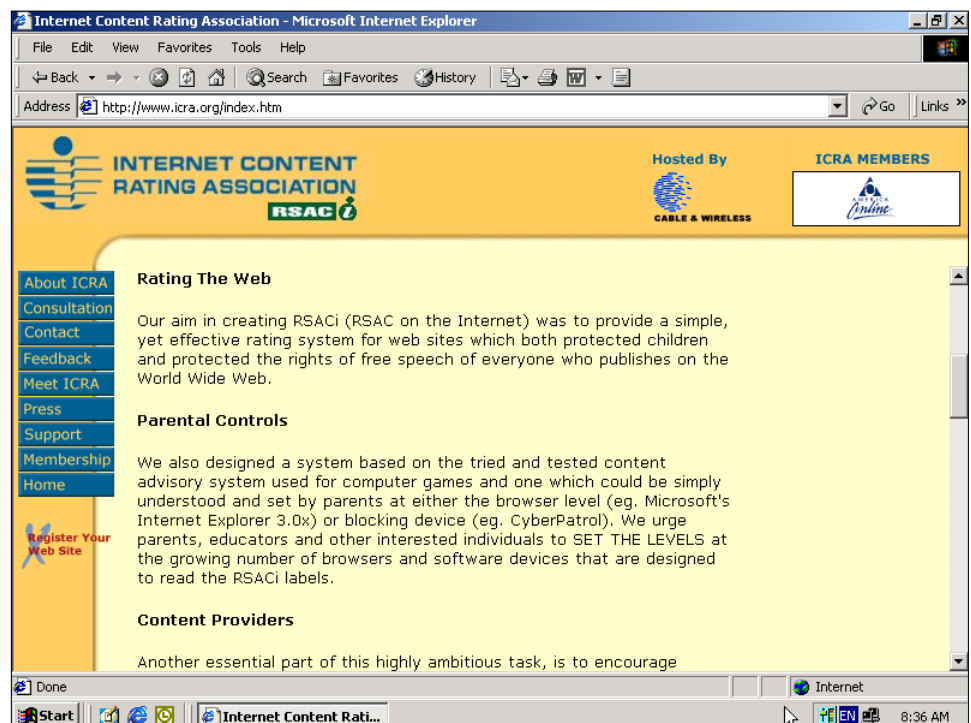


Figure 12-38 Many Web browsers use the ratings of the RSACi (Recreational Software Advisory Council for the Internet), which allows you to specify a rating level for material unsuitable for minors.

Web site. Concerned parents can set the rating limits and prevent these limits from being changed by using a password.

Another approach is to use Web filtering software. **Web filtering software**, also called an **Internet filtering program**, is software that can restrict access to specified Web sites. Some also filter sites that use specific words. Others allow you to filter e-mail messages and chat rooms.

CHAPTER SUMMARY

This chapter identified some potential risks to computers and software and the safeguards that schools, businesses, and individuals can implement to minimize these risks. Internet security risks and safeguards also were discussed. The chapter also presented actions you can take to keep your personal data private.



Privacy Online

The loss of personal privacy is a major concern of many Americans. Concerns about loss of privacy are not new, but the computer's ability to gather and sort vast amounts of data — and the Internet's ability to distribute it globally — magnifies those concerns. It is difficult to be anonymous once you have ventured onto the Internet. You can expect to receive unsolicited advertising via e-mail and even personalized ads that seem to know you. This so-called junk e-mail can be a nuisance, even a scam. The Online Privacy Organization (see URL below) guidelines for Web sites are as follows: "The policy should clearly state what information is being collected; the use of that information; possible third party distribution of that information; the choices available to an individual regarding collection, use and distribution of the collected information; a statement of the organization's commitment to data security; and what steps the organization takes to ensure data quality and access." So how do you protect yourself online?

- If you are going to provide personal information through an online form, verify that the Web site has a privacy policy. The policy should be easy to find and should follow the guidelines of the Online Privacy Organization.
- If you are providing information to one of the three major credit bureaus, request that your personal information not be shared with others or used for promotional purposes.
- Some state Department of Motor Vehicles (DMV) distribute your personal information for direct marketing. The Federal Drivers Protection Act (see URL below) gives you privacy rights concerning your personal information. Contact the DMV in your state to find out if your personal information is sold for direct marketing purposes.
- The Direct Marketing Association (DMA) (see URL below) offers services that allow you to opt-out of direct marketing from many national companies. This includes e-mail advertising. Fill out the forms online at the DMA Web site.
- Use filtering software for children.
- Look for third party seals, such as the TRUSTe trustmarks.
- Some other tips are as follows:
 - Use a screen name when participating in chat rooms.
 - Set your browser to let you make the decision regarding cookie files being saved to your computer.
 - Do not send your credit card number or other sensitive, personal data by e-mail unless you are assured that the data is encrypted with the latest software technology.
 - Be cautious about giving out your Social Security number or credit card number.

For more information on protecting yourself online, privacy issues, and the Web sites mentioned above, visit the Discovering Computers 2002 Apply It Web page (scsite.com/dc2002/apply.htm) and click Chapter 12 Apply It #3.



Network Security Specialist

Employment as a network security specialist requires a technical background, including a thorough understanding of industry-standard network design practices and tools. Hands-on experience configuring routers and firewalls is a necessity. Many companies require a strong knowledge of Web protocols and enterprise technologies.

Certification within the networking security field is not as defined and as well known as other IT certifications. The following includes some certification examples:

- Checkpoint — offers certification in three different categories, including Certified Security Administrator (CSA), Certified Security Engineer (CSE), and Certified Senior Security Specialist (CSSS) (see URL below).
- IBM — provides certification opportunities for their IBM SecureWay Firewall for Windows (see URL below).
- The International Information Systems Security Certification Consortium, Inc. — developed a Certified Information Systems Security Professional examination (see URL below).
- Learning Tree — provides three courses in System and Network Security (see URL below).

Salaries for network security specialists are generally in the \$75,000 and up range. To work within this technical field requires prior network knowledge and experience. Certification is a plus, although most of the existing certification programs are very specialized.

To learn more about the field of network security as a career and for links to the Web sites mentioned above, visit the Discovering Computers 2002 Careers Web page (scsite.com/dc2002/careers.htm) and click Network Security Specialist.

E-ENVIRONMENT

THE FATE OF THE ENVIRONMENT

Protecting the Planet's Ecosystem

The figures are startling: Each year Americans consume 1.4 trillion sheets of paper, an increase of 76 percent since 1980. In the past 50 years, people have consumed as many natural resources as every human who has ever lived. According to The Center for a New American Dream (Figure 12-39), the U.S. Postal Service's letter carriers deliver an average of 17.8 tons of junk mail each year, which is the weight of four male elephants.

From the rain forests of Africa to the marine life in the Pacific Ocean, the fragile ecosystem is under extreme stress. Many environmental groups have developed Internet sites in attempts to educate worldwide populations and to increase resource conservation.

The U.S. Government has a number of Web sites devoted to specific environmental concerns. For example, the U.S. Geological Survey monitors the chemicals found in acid rain and conducts research to analyze the effects of these atmospheric deposits on aquatic and terrestrial ecosystems. Figure 12-40 shows the home page for the Central African Regional Program for the Environment (CARPE). This continuing project of the U.S. Agency for International Development protects the Congo Basin's tropical forests from population growth, deforestation, and other economic and political problems. In another Web site, the U.S. Environmental Protection Agency (EPA) provides pollution data, including ozone levels and air pollutants, for specific



Figure 12-39 The Center for a New American Dream Web site provides an area where you can declare your independence from junk mail and get your address removed from bulk mail lists.

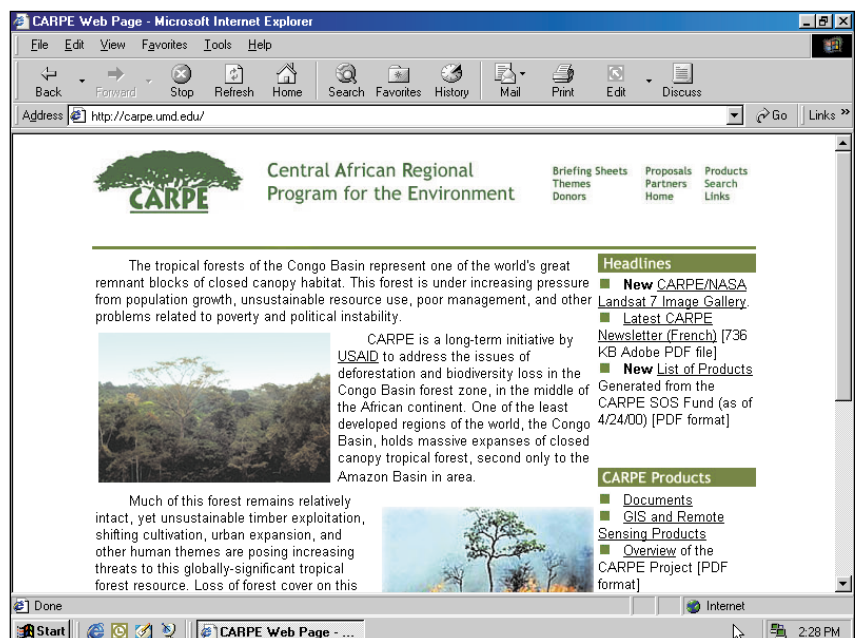


Figure 12-40 The Congo Basin's ecological, economic, and political issues are discussed in the CARPE Web site.

areas. Its Aerometric Information Retrieval System (AIRS) database, shown in Figure 12-41, is the world's most extensive collection of air pollution data.

On an international scale, the Environmental Sites on the Internet (Figure 12-42) Web page developed by the Royal Institute of Technology in Stockholm, Sweden, has been rated as one of the best ecological sites. Its comprehensive listing of environmental concerns range from aquatic ecology to wetlands.

For more information on environment Web sites, visit the Discovering Computers 2002 E-Revolution Web page (scs.site.com/dc2002/e-rev.htm) and click Environment.

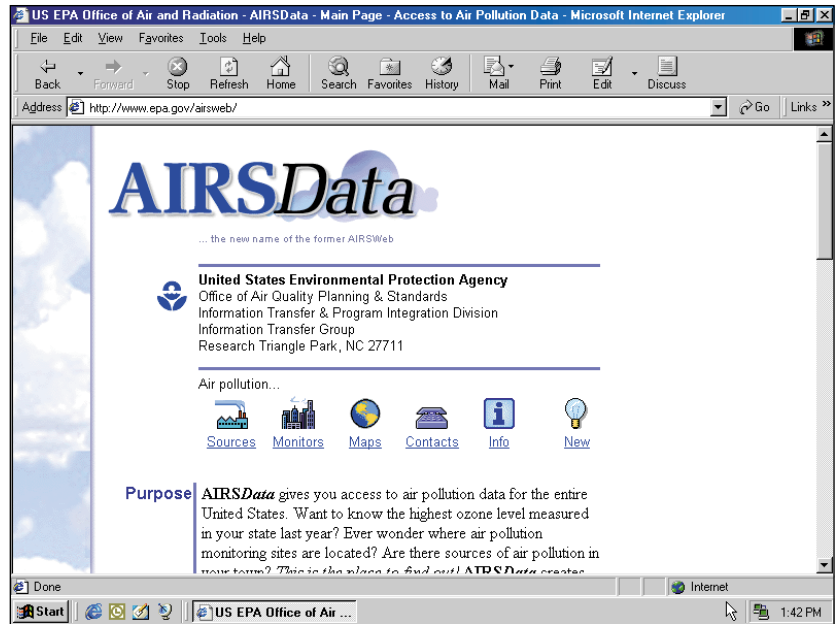


Figure 12-41 A visit to the AIRSData Web site, with its extensive database, can assist you in checking your community's ozone and air pollutant levels.

ENVIRONMENT WEB SITES	URL
Central African Regional Program for the Environment (CARPE)	carpe.umd.edu
EarthJustice Legal Defense Fund	www.earthjustice.org
Environmental Defense	edf.org
Environmental Sites on the Internet	www.lib.kth.se/~lg/envsite.htm
Green Solitaire	greensolitaire.bizland.com
GreenNet	www.gn.apc.org
Lycos Environment News	ens-news.com
The Center for a New American Dream	newdream.org
The World Wide Web Virtual Library of Ecology & Biodiversity	conbio.rice.edu/vl
U.S. EPA, Office of Air and Radiation	www.epa.gov/airsweb
U.S. Geological Survey (USGS), Acid Rain Data and Reports	btdqs.usgs.gov/acidrain
UWM Environmental Health, Safety, & Risk Management	www.uwm.edu/Dept/EHSRM/EHSLINKS

For an updated list of environment Web sites, visit scs.site.com/dc2002/e-rev.htm.

Figure 12-42 Environmental Web sites provide vast resources for ecological data and action groups.

E-ENVIRONMENT

applied:

1. The Center for a New American Dream Web site encourages consumers to reduce the amount of junk mail sent to their homes. Using the table in Figure 12-42, visit the Web site and write a paragraph stating how many trees are leveled each year to provide paper for these mailings, how many garbage trucks are needed to haul this waste, and other statistics. Read the letters that you can use to eliminate your name from bulk mail lists. To whom would you mail these letters? How long does it take to stop these unsolicited letters?
2. Visit the AIRSData Web site. What is the highest ozone level recorded in your state this past year? Where are the nearest air pollution monitoring Web sites, and what are their levels? Where are the nearest sources of air pollution? Read two reports on two different topics, such as acid rain and air quality, and summarize their findings. Include information on who sponsored the research, who conducted the studies, when the data was collected, and the impact of this pollution on the atmosphere, water, forests, and human health. Whom would you contact for further information regarding the data and studies?

In Summary

Student Exercises
[Web Links](#)
[In Summary](#)
[Key Terms](#)
[Learn It Online](#)
[Checkpoint](#)
[In The Lab](#)
[Web Work](#)
Special Features ■ [TIMELINE 2002](#) ■ [WWW & E-SKILLS](#) ■ [MULTIMEDIA](#) ■ [BUYER'S GUIDE 2002](#) ■ [WIRELESS TECHNOLOGY](#) ■ [TRENDS 2002](#) ■ [INTERACTIVE LABS](#) ■ [TECH NEWS](#)

 **Web Instructions:** To display this page from the Web, start your browser and enter the URL scs.site.com/dc2002/ch12/summary.htm. Click the links for current and additional information. To listen to an audio version of this In Summary, click the Audio button. To play the audio, RealPlayer must be installed on your computer (download by clicking [here](#)).

1

What Are the Various Types of Security Risks that Can Threaten Computers?

A **computer security risk** is any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability. [Computer security risks](#) include computer viruses, unauthorized access and use, hardware theft, software theft, information theft, and system failure. A computer **virus** is a potentially damaging computer program designed to affect or infect a computer negatively by altering the way it works. **Unauthorized access** is the use of a computer or network without permission; **unauthorized use** is the use of a computer or its data for unapproved or possibly illegal activities. An individual who tries to access a computer or network illegally is called a [cracker](#) or a **hacker**. **Hardware theft**, software theft, and **information theft** present difficult security challenges. The most common form of software theft is **software piracy**, which is the unauthorized and illegal duplication of copyrighted software. A **system failure** is the prolonged malfunction of a computer.

2

How Can a Computer Be Safeguarded?

Safeguards are protective measures that can be taken to minimize or prevent the consequences of computer security risks. An **antivirus program** protects a computer against viruses by identifying and removing any computer viruses found in memory. An **access control** prevents unauthorized access and use by defining who can access a computer, when they can access it, and what actions they can take. Physical access controls and common sense can minimize hardware theft. For an organization, a **site license** addresses software piracy by giving the buyer the right to install the software on multiple computers at a single site. [Encryption](#) reduces information theft by converting readable data into unreadable characters. A **surge protector** and an **uninterruptible power supply** guard against system failure by controlling power irregularities.

3

How Does a Computer Virus Work and What Steps Can Be Taken to Prevent Viruses?

A [virus](#) is a potentially damaging computer program that affect, or infects, a computer negatively by altering the way the computer works. A virus can replace the boot program with an infected version (**boot sector virus**), attach itself to a file (**file virus**), or use an application's macro language to hide virus code (**macro virus**). Other viruses are activated when a certain action takes place or condition is met (**a logic bomb**) or on a specific date (**a time bomb**). A **malicious-logic program**, or **malware**, is a program that acts without a user's knowledge and deliberately alters the computer's operations. These include programs that copy themselves repeatedly in memory (**worm**), or viruses that hide within a legitimate program (**Trojan horse**). Viruses can be prevented by installing an antivirus program, setting the macro security level in all applications, write-protecting a **rescue disk** or **emergency disk**, never starting a computer with a disk in drive A, scanning floppy disks for viruses, checking downloaded programs, and regularly backing up files.

4

How Can an Individual Create a Good Password?

A [password](#) is a secret combination of characters associated with the **user name** that allows access to certain computer resources. With most systems, you can select your own password. Passwords are effective only if they are chosen carefully and are impossible to guess. Guidelines to ensure secure passwords include using at least eight characters; using a combination of numbers, letters, words, initials, and dates; and choosing a combination that only you would know. To safeguard your password, do not write it down or share it. Choose a password that you can type easily without looking at the keyboard, and change your password frequently.

In Summary

Student Exercises

Web Links

In Summary

Key Terms

Learn It Online

Checkpoint

In The Lab

Web Work

Special Features ■ **TIMELINE 2002** ■ **WWW & E-SKILLS** ■ **MULTIMEDIA** ■ **BUYER'S GUIDE 2002** ■ **WIRELESS TECHNOLOGY** ■ **TRENDS 2002** ■ **INTERACTIVE LABS** ■ **TECH NEWS**

5

What Are Various Biometric Devices?

A **biometric device** authenticates a person's identity by verifying personal characteristics. They are used to access programs, systems, or rooms using computer analysis of some **biometric identifier**. Examples of biometric identifiers include a **fingerprint scanner**, a **hand geometry system**, and a **face recognition system**, a **voice verification system**, a **signature verification system**, and an **iris recognition system**.

6

What Is Software Piracy?

Software piracy is the unauthorized and illegal duplication of copyrighted software and is the most common form of software theft. When people purchase software, they purchase a license agreement for the right to use the software. Users are permitted to install the software on only one computer, make one backup copy, and give or sell the software to another person if they remove it from their computers.

7

Why Is Encryption Necessary?

Encryption converts readable data into unreadable characters to prevent unauthorized access. The two basic types of encryption are **private key encryption**, where both the originator and recipient use the same secret key; and **public key encryption**, where a public key is known to everyone and a private key is known only by the sender or receiver. **RSA encryption** is a public key encryption technology used to encrypt data transmitted over the Internet, and **Fortezza** is a public key encryption technology that stores user information on a PC Card.

8

Why Is Computer Backup Important and How Is It Accomplished?

A **backup** is a duplicate of a file, program, or disk that can be used if the original is lost, damaged, or destroyed. In case of **system failure** or the discovery of corrupted files, the backup can be used to **restore** the files by copying the backed up files to their original location on the computer. **Backup procedures** specify a regular plan of copying and storing important data and program files. Three methods of backup are: a **full backup**, a **differential backup**, and an **incremental backup**.

9

What Are the Steps in a Disaster Recovery Plan?

A **disaster recovery plan** describes the steps an organization would take to restore computer operations in the event of a disaster and has four major components: the **emergency plan**, the **backup plan**, the **recovery plan**, and the **test plan**.

10

What Are the Ways to Secure an Internet Transaction?

Information transmitted over the Internet has a high degree of security risk. **Secure sites** use encryption techniques to secure data. To provide secure data transmission, Web browsers use encryption technology such as **Secure Socket Layers (SSL)** and **digital signatures**. Netscape Navigator and Microsoft Internet Explorer use RSA. The **Secure Electronic Transaction (SET)** uses a public key encryption to secure credit card transaction systems.

11

What Are Issues Pertaining to Personal Information?

Information privacy refers to the right of individuals and organizations to deny or restrict the collection and use of information about them. Information privacy issues include unauthorized collection and use of information and employee monitoring. Unauthorized collection and use of information involves the compilation of data about an individual from a variety of sources. A **cookie** is a small file that a Web server stores on your computer that contains data about you. Web sites use cookies to track user preferences, how often you visit a Web site and Web pages visited; to store your password; to keep track of items you purchase (**session cookie**); and to target advertisements. **Spyware** is a program that communicates information to some outside source while you are online. It is placed on your computer without your knowledge and can enter your computer as a virus or as a result of installing a new program. **Employee monitoring** involves the use of computers to observe, record, and review an individual's use of a computer, including communications, keyboard activity, and Internet sites visited.

Key Terms

Student Exercises
[Web Links](#)
[In Summary](#)
[Key Terms](#)
[Learn It Online](#)
[Checkpoint](#)
[In The Lab](#)
[Web Work](#)
Special Features ■ [TIMELINE 2002](#) ■ [WWW & E-SKILLS](#) ■ [MULTIMEDIA](#) ■ [BUYER'S GUIDE 2002](#) ■ [WIRELESS TECHNOLOGY](#) ■ [TRENDS 2002](#) ■ [INTERACTIVE LABS](#) ■ [TECH NEWS](#)

Web Instructions: To display this page from the Web, start your browser and enter the URL scsite.com/dc2002/ch1/terms.htm. Scroll through the list of terms. Click a term to display its definition and a picture. Click the To WEB button for current and additional information about the term from the Web. To see animations, Shockwave and Flash Player must be installed on your computer (download by clicking [here](#)).

access control (12.8)
adware (12.31)
anti-spam program (12.31)
antivirus program (12.5)
archival backup (12.20)
asymmetric key encryption (12.17)
audit trail (12.13)
authentication (12.8)
back up (12.19)
backup (12.19)
backup plan (12.21)
backup procedures (12.20)
biometric device (12.10)
biometric identifier (12.10)
blackout (12.18)
boot sector virus (12.4)
brownout (12.18)
Business Software Alliance (BSA) (12.15)
callback system (12.12)
certificate authority (CA) (12.23)
child (12.21)
ciphertext (12.16)
Clipper chip (12.17)
Communications Decency Act (12.34)
computer crime (12.2)
Computer Fraud and Abuse Acts (12.32)
Computer Matching and Privacy Protection Act (12.32)
computer security plan (12.22)
computer security risk (12.2)
cookie (12.28)
cracker (12.7)
cybercrime (12.2)
data encryption standard (DES) (12.16)
decrypt (12.16)
differential backup (12.20)
digital certificate (12.23)
digital ID (12.24)
digital signature (12.24)
disaster recovery plan (12.21)
Electronic Communications Privacy Act (ECPA) (12.32)
e-mail filtering (12.31)
emergency disk (12.6)
emergency plan (12.21)
employee monitoring (12.33)
encryption (12.16)
encryption key (12.16)
end-user license agreement (EULA) (12.14)
face recognition system (12.11)
Fair Credit Reporting Act (12.33)
file virus (12.4)
fingerprint scanner (12.11)
firewall (12.24)
Fortezza (12.17)
full backup (12.20)
grandparent (12.21)

hacker (12.7)
hand geometry system (12.11)
hardware theft (12.13)
hardware vandalism (12.13)
hash (12.24)
identification (12.8)
incremental backup (12.20)
information privacy (12.26)
information theft (12.15)
inoculate (12.6)

POSSESSED OBJECT

An item, such as a badge, card, or key, that must be carried to gain access to a computer or computer facility. The card that allows access to an ATM is an example of a possessed object. (12.10)



International Computer Security Association (ICSA) (12.22)
Internet filtering program (12.35)
iris recognition system (12.12)
issuing authority (IA) (12.23)
Joule (12.19)
key escrow (12.17)
license agreement (12.14)
log (12.13)
logic bomb (12.4)
macro virus (12.4)
malicious-logic program (12.4)
malware (12.4)
network site license (12.15)
noise (12.18)
offsite (12.19)
online backup service (12.21)
online security service (12.26)
overvoltage (12.18)
parent (12.21)
password (12.8)
personal firewall (12.25)
personal identification number (PIN) (12.10)

plaintext (12.16)
polymorphic virus (12.6)
possessed object (12.10)
power surge (12.18)
Pretty Good Privacy (PGP) (12.24)
Privacy for Consumers and Workers Act (12.33)
private key encryption (12.16)
program virus (12.4)
proxy server (12.25)
public key encryption (12.17)
public-key certificate (12.23)
quarantine (12.6)
reciprocal backup relationship (12.21)
recovery plan (12.21)
rescue disk (12.6)
restore (12.19)
RSA encryption (12.17)
safeguards (12.2)
Secure Electronic Transaction (SET) (12.24)
Secure HTTP (S-HTTP) (12.24)
secure site (12.23)
Secure Sockets Layer (SSL) (12.24)
session cookie (12.29)
signature verification system (12.12)
single-user license agreement (12.14)
site license (12.15)
software piracy (12.14)
spam (12.31)
spike (12.18)
spyware (12.31)
stealth virus (12.6)
surge protector (12.18)
surge suppressor (12.18)
symmetric key encryption (12.16)
system failure (12.18)
system virus (12.4)
test plan (12.21)
three-generation backup (12.21)
time bomb (12.4)
Trojan horse (12.4)
trusted source (12.2)
unauthorized access (12.7)
unauthorized use (12.7)
undervoltage (12.18)
Underwriters Laboratories (UL) 1449 standard (12.19)
uninterruptible power supply (UPS) (12.19)
user ID (12.8)
user name (12.8)
virus (12.2)
virus author (12.2)
virus definition (12.6)
virus hoax (12.7)
virus signature (12.6)
voice verification system (12.12)
Web filtering software (12.35)
worm (12.4)

Learn It Online

Student Exercises

Web Links

In Summary

Key Terms

Learn It Online

Checkpoint

In The Lab

Web Work

Special Features

■ TIMELINE 2002 ■ WWW & E-SKILLS ■ MULTIMEDIA ■ BUYER'S GUIDE 2002 ■ WIRELESS TECHNOLOGY ■ TRENDS 2002 ■ INTERACTIVE LABS ■ TECH NEWS

Web Instructions: To display this page from the Web, start your browser, and then enter the URL scsite.com/dc2002/ch12/learn.htm.

1. Web Guide

Click [Web Guide](#) to display the Guide to World Wide Web Sites and Searching Techniques Web page. Click Computers and Computing. Click Government and Politics and then click Electronic Frontier. Click one of the Recent News links and review the information. Use your word processing program to prepare a brief report on what you learned and submit your assignment to your instructor.

2. Scavenger Hunt

Click [Scavenger Hunt](#). Print a copy of the Scavenger Hunt page; use this page to write down your answers as you search the Web. Submit your completed page to your instructor.

3. Who Wants to Be a Computer Genius?

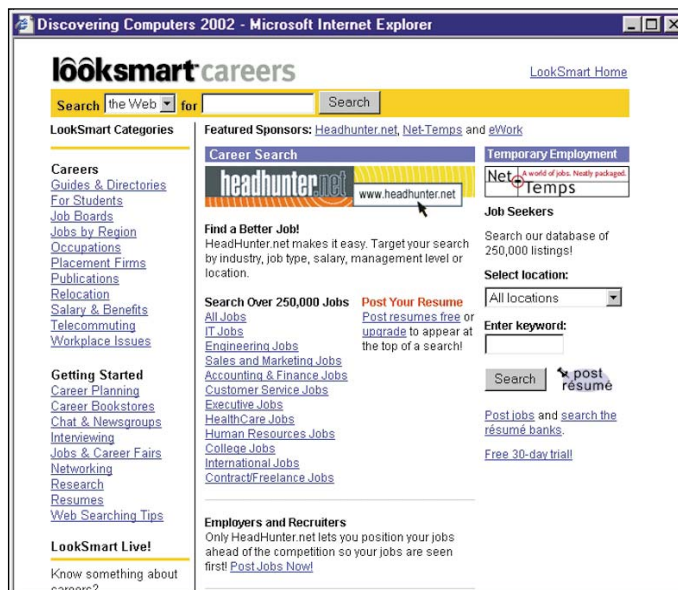
Click [Computer Genius](#) to find out if you are a computer genius. Directions on how to play the game will display. When you are ready to play, click the PLAY button. Submit your score to your instructor.

4. Wheel of Terms

Click [Wheel of Terms](#) to reinforce important terms you learned in this chapter by playing the Shelly Cashman Series version of this popular game. Directions on how to play the game will display. When you are ready to play, click the PLAY button. Submit your score to your instructor.

5. Career Corner

Click [Career Corner](#) to display the Career Center page. Review this page. Click one of the Online Job Bank links. Write a brief report on what you discovered. Submit the report to your instructor.



6. Search Sleuth

Click [Search Sleuth](#) to learn search techniques that will help make you a research expert. Submit the completed assignment to your instructor.

7. Crossword Puzzle Challenge

Click [Crossword Puzzle Challenge](#). Complete the puzzle to reinforce skills you learned in this chapter. Directions on how to play the game will display. When you are ready to play, click the PLAY button. Submit the completed puzzle to your instructor.

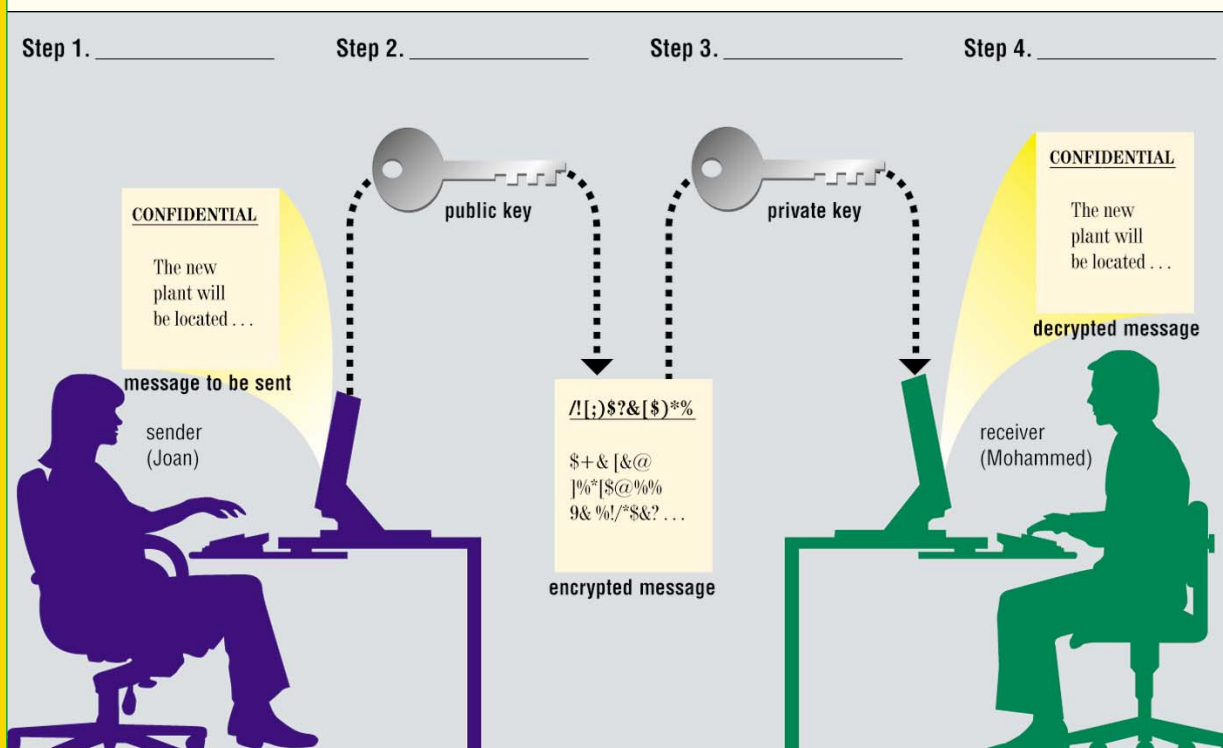
8. Practice Test

Click [Practice Test](#). Answer each question. When completed, enter your name and click the Grade Test button to submit the quiz for grading. Make a note of any missed questions. If required, print a copy to submit to your instructor.

Checkpoint

Student Exercises
[Web Links](#)
[In Summary](#)
[Key Terms](#)
[Learn It Online](#)
[Checkpoint](#)
[In The Lab](#)
[Web Work](#)
Special Features ■ [TIMELINE 2002](#) ■ [WWW & E-SKILLS](#) ■ [MULTIMEDIA](#) ■ [BUYER'S GUIDE 2002](#) ■ [WIRELESS TECHNOLOGY](#) ■ [TRENDS 2002](#) ■ [INTERACTIVE LABS](#) ■ [TECH NEWS](#)

Web Instructions: To display this page from the Web, start your browser and enter the URL scsite.com/dc2002/ch12/check.htm. Click the links for current and additional information. To experience the animation and interactivity, Shockwave and Flash Player must be installed on your computer (download by clicking [here](#)).


LABEL THE FIGURE
Instructions: Identify the steps showing how public key encryption works.

MATCHING
Instructions: Match each term from the column on the left with the best description from the column on the right.

- _____ 1. digital certificate
- _____ 2. possessed object
- _____ 3. voice verification system
- _____ 4. password
- _____ 5. callback system

- a. Compares a person's live speech to his or her stored [voice pattern](#).
- b. [Encrypted code](#) that a person, Web site, or company attaches to an electronic number (PIN) message.
- c. Connects to a [computer](#) only after the computer calls back at a previously established number.
- d. A notice that guarantees a [user](#) or a Web site is legitimate.
- e. A secret combination of characters associated with the user name that allows access to certain [computer resources](#).
- f. Item that must be carried to gain access to a computer or [computer facility](#).
- g. Uses special electrical components to smooth out minor [noise](#) and provide a stable flow.

Checkpoint

Student Exercises

Web Links

In Summary

Key Terms

Learn It Online

Checkpoint

In The Lab

Web Work

Special Features ■ TIMELINE 2002 ■ WWW & E-SKILLS ■ MULTIMEDIA ■ BUYER'S GUIDE 2002 ■ WIRELESS TECHNOLOGY ■ TRENDS 2002 ■ INTERACTIVE LABS ■ TECH NEWS



MULTIPLE CHOICE

Instructions: Select the letter of the correct answer for each of the following questions.

1. A(n) _____ is a company or person you believe will not send you a [virus-infected file](#) knowingly.
 - a. trusted source
 - b. antivirus author
 - c. certificate authority
 - d. grandparent
2. A [security](#) option that authenticates someone's identity by verifying personal characteristics is called a _____.
 - a. digital signature
 - b. PIN
 - c. possessed object
 - d. biometric device
3. Illegal duplication of [copyrighted software](#) is referred to as _____.
 - a. software piracy
 - b. software vandalism
 - c. information theft
 - d. site license removal
4. A _____ [virus](#) executes when you turn on the computer.
 - a. file
 - b. boot
 - c. macro
 - d. time bomb
5. A(n) _____ tries to access a computer or [computer network](#) illegally.
 - a. hacker
 - b. unidentified user
 - c. auditor
 - d. software tester



SHORT ANSWER

Instructions: Write a brief answer to each of the following questions.

1. In terms of computer viruses, how is a [logic bomb](#) different from a time bomb? _____
What is a worm? _____ What are some other types of viruses? _____
2. What is an Internet security risk? _____ What are some [security techniques](#)? _____
3. What is a computer [security plan](#)? _____ What are the three steps for a security plan? _____
4. How is [private key encryption](#) different from public key encryption? _____ What is the government's key escrow plan? _____ What are two types of public key encryption? _____
5. What is a [password](#)? _____ How can you create a good password? _____
What are some password precautions? _____



WORKING TOGETHER

Instructions: Working with a group of your classmates, complete the following team exercise.

Your group has been hired by XYZ Corporation to create a [privacy information policy](#) for an online Web site for the company. Directions include putting together a policy that not only will respect an individual's privacy rights, but also will enable the company to collect data that can be used in targeted marketing. The company would like to know who visits the Web site, how often they visit, what pages are viewed, and how long someone stays on a particular page. Create a privacy policy that will include all of the above. Justify each component within the policy and explain how the policy will not violate the individual's right to privacy. Share your report and/or a PowerPoint presentation with the class.

In The Lab

Student Exercises
[Web Links](#)
[In Summary](#)
[Key Terms](#)
[Learn It Online](#)
[Checkpoint](#)
[In The Lab](#)
[Web Work](#)
Special Features
[TIMELINE 2002](#) [WWW & E-SKILLS](#) [MULTIMEDIA](#) [BUYER'S GUIDE 2002](#) [WIRELESS TECHNOLOGY](#) [TRENDS 2002](#) [INTERACTIVE LABS](#) [TECH NEWS](#)

Web Instructions: To display this page from the Web, start your browser and enter the URL scsite.com/dc2002/ch12/lab.htm. Click the links for current and additional information.

Understanding Backup



This exercise uses Windows 98 or Windows 2000 procedures. Click the Start button on

the taskbar, point to Programs on the Start menu, and then point to Accessories on the Programs submenu. Point to System Tools on the Accessories submenu, and then click Backup on the System Tools submenu. If a Welcome screen displays, click the Close button. When the Microsoft Backup - [Untitled] window displays, maximize it and then click the Backup tab. Click Help on the menu bar and then click Help Topics. If necessary, click the Contents tab. Click Back Up, and then click Backing Up Everything On Your Computer. How can you [backup](#) your system? Close the Backup Help window. Close the Microsoft Backup - [Untitled] window.



License Agreements

This exercise uses Windows 98 or Windows 2000

procedures. Click the Start button on the taskbar. Click Help on the Start menu. If necessary, click the Contents tab. Click the Introducing Windows 98 or Windows 2000 book. Click the Register Your Software book. Click the License Agreement questions and

answers topic. Click an appropriate link to answer each of the following questions:

- Where do you find your [End User License Agreement](#)?
- Is it legal to sell software you have bought and used?
- Can you make a second copy of software for a home or notebook computer?
- Can you transfer or give away old versions of products when you buy an upgrade?

Click the Close button to close Windows Help.

Scanning a Disk



This exercise uses Windows 98 procedures. ScanDisk is a Windows utility that checks a disk for [physical and logical errors](#).

To run ScanDisk, click the Start button on the taskbar, point to Programs on the Start menu, and then point to Accessories on the Programs submenu. Point to System Tools on the Accessories submenu, and then click ScanDisk on the System Tools submenu. Click the Advanced button in the ScanDisk window. When the ScanDisk Advanced Options dialog box displays, if necessary click Always in the Display summary area and then click the OK button. Insert your floppy disk into drive A. Click 3½ Floppy (A:) in the Select the

drive(s) you want to check for errors list. Click the Thorough option button in the Type of test area. Click the Start button in the ScanDisk - 3½ Floppy (A:) window. What errors, if any, are detected? In bytes, what is the total disk space? How many folders are on the floppy disk? How many user files are on the floppy disk? Close the ScanDisk Results dialog box and the ScanDisk - 3½ Floppy (A:) window.



Checking System Resources

This exercise uses Windows 98

procedures. [Resource Meter](#) monitors the system resources your programs are using. To run Resource Meter, click the Start button on the taskbar, point to Programs on the Start menu, and then point to Accessories on the Programs submenu. Point to System Tools on the Accessories submenu, and then click Resource Meter on the System Tools submenu. If a Resource Meter dialog box displays, read the information and then click the OK button. Double-click the Resource Meter icon that displays to the left of the time on the taskbar. What percentage of system resources is free? What percentage of user resources is free? Click the OK button. Right-click the Resource Meter icon on the taskbar and then click Exit on the shortcut menu.

Web Work

Student Exercises

Web Links

In Summary

Key Terms

Learn It Online

Checkpoint

In The Lab

Web Work

Special Features ■ TIMELINE 2002 ■ WWW & E-SKILLS ■ MULTIMEDIA ■ BUYER'S GUIDE 2002 ■ WIRELESS TECHNOLOGY ■ TRENDS 2002 ■ INTERACTIVE LABS ■ TECH NEWS

Web Instructions: To display this page from the Web, start your browser and enter the URL scsite.com/dc2002/ch12/web.htm. To view At The Movies in exercise 1, RealPlayer must be installed on your computer (download by clicking [here](#)). To use the Shelly Cashman Series Keeping Your Computer Virus Free Lab from the Web, Shockwave and Flash Player must be installed on your computer (download by clicking [here](#)).



Workplace Watchdog

To view the Workplace Watchdog movie, click the button to the left or click the Play button to the right. Watch the movie, and then complete the exercise by answering the questions below. Increasingly, companies are installing computer surveillance software to monitor and record all employee activities on the computer. One employer discovered that several employees were spending 50 to 70 percent of their time playing games, sending personal e-mail, and surfing the Web. So far the courts have said that, because the employer owns the computers, workplace surveillance is okay, provided employees are forewarned of the policy. Does the employee have any right to privacy on the company's computer? Can the employer record employee telephone calls? Do employees have the right make private cellular telephone calls on company property? Can a company use video surveillance in the factory, lunchroom, or rest rooms?



Shelly Cashman Series Keeping Your Computer Virus Free Lab

Follow the instructions in Web Work 2 on page 1.47 to start and use the Shelly Cashman Series Keeping Your Computer Virus Free Lab. If you are running from the Web, enter the URL www.scsite.com/scslabs/menu.htm; or display the Web Work page (see instructions at the top of this page) and then click the button to the left.



Software Piracy

Hong Kong once was the pirated software capital of the world. The availability of stolen software manufactured in China and smuggled across the border led to the use of pirated software by almost 65 percent of Hong Kong firms. To date, the impact of China's takeover of Hong Kong on the pirated software market is unknown. The Business Software Alliance (BSA) Web site provides the latest information about software piracy. To learn more, click the button to the left and complete this exercise.



Computer Crime

The Federal Bureau of Investigation is taking computer crime seriously. The FBI has computer crime units in several cities, and a team of 125 agents is responsible for coordinating investigations around the country. Part of their job is to anticipate, and prevent, the most catastrophic crimes computer crackers could commit. Many computer crimes fall under the jurisdiction of the FBI. To learn more about the computer crimes the FBI investigates, click the button to the left and complete this exercise.



In the News

Carnivore is the name of an electronic surveillance tool used by the FBI to monitor the e-mail communications of suspected criminals and other people under investigation. Many consider this Internet wiretapping because the program must read all e-mail address information that passes through an ISP in order to work. Click the button to the left and read a news story about a security, ethics, or privacy issue related to computers. What is the issue? Who does it affect? How do you think the issue can, or should, be resolved?

